2018

Through the Net: Investigating How User Characteristics Influence Susceptibility to Phishing

Charlie Marriott
Technological University Dublin

Through The Net: Investigating How User Characteristics Influence Susceptibility To Phishing

Charlie Marriott
D14123014

A dissertation submitted in partial fulfilment of the requirements of
Dublin Institute of Technology for the degree of M.Sc. in Computing (Security & Forensics)

June 2018

Declaration

I certify that this dissertation which I now submit for examination for the award of M.Sc. in Computing (Forensics and Security), is entirely my own work and has not been taken from the work of others save and to the extent that such work has been cited and acknowledged within the text of my work.

This dissertation was prepared according to the regulations for postgraduate study of the Dublin Institute of Technology and has not been submitted in whole or part for an award in any other Institute or University.

The work reported on in this dissertation conforms to the principles and requirements of the Institute's guidelines for ethics in research.

Signed: 

Date: 13/06/2018

Abstract

In the past 25 years, the internet has grown and evolved from a niche networking technology, used almost exclusively by researchers and enthusiasts, into the driving force of modern economies. Fraud has evolved too, with rates of cybercrime on the increase as criminals become increasingly sophisticated in using technology to deceive their victims. The world is an online place, and data is the new oil.

Phishing is a form of social engineering that is not that different from traditional fraud. Phishing attackers try to trick their victims into revealing valuable private information, usually for financial gain, by posing as a legitimate, trusted entity through the use of technical and content-related deceptions. There have been several high profile data breaches in the last number of years, and these usually begin with a successful phishing attack. At the other end of the spectrum, private individuals regularly fall victim to smaller phishing crimes, the majority of which are never reported.

A lot of research has been done to identify exactly who falls for a phishing scam, identifying four categories: 1. Demographics, 2. Experience, 3. Attitude to Privacy and 4. Computer Self-Efficacy. The existing body of knowledge, however, is inconclusive regarding what groups within these categories are most at risk.

This study seeks to better understand what factors influence a person's susceptibility to phishing attacks, revisiting existing research but in a climate where even the most basic internet user is now aware of cybercrime and using a large and diverse sample of participants. In addition, the study investigates if respondents from different groups rely more or less on technical or non-technical slues when evaluating the legitimacy of an email.

The study was conducted over a period of several weeks, and over two hundred participants completed a survey and phishing test where they were asked to evaluate the legitimacy of ten emails presented as screenshots and accompanied by a scenario describing the context within which the email was received. The results of the survey and test were analysed to identify any statistically significant information.

Results from the study indicate that factors of demographics and computer self-efficacy may have a significant impact on user susceptibility to phishing. Information regarding the relevance of experience and attitude to privacy were inconclusive. The investigation into how respondents were processing information found no significant difference between the best and worst performers across all categories however the group of respondents, as a whole, were more successful at identifying content-based deception over technical deception by a marginal amount.

Acknowledgements

I would like to thank my wife Áine, my daughter Emily and my son Oliver, for their love and unending support. I could not have completed this without your patience, understanding and cups of coffee.

I would like to thank the faculty and staff at DIT, not only for their advice and assistance along the way but for the kindness and consideration I was afforded when I suffered a bereavement during the completion of the program.

Special thanks go to my friends and colleagues who supported me on this journey and lobbied their networks to participate. In particular, Paul O'Connor, David Power, Donal O'Donovan and Claire Walsh for talking me down when it was necessary.

Thank you to Eir and Damien Duffy, my former manager, for all the support when I was trying to get back into this college thing after 20 years, and to Integrity360 for all the encouragement.

I would like to thank my supervisor, Patrick Tobin, for his contributions and support through the process.

Last but not least, a special thank you to my late father, John, without whom none of this would have been possible.

Table of Contents

Table of Figures

Table of Tables

1. Introduction

1.1. Background

A phishing attack is a type of social engineering that seeks to trick individuals into releasing sensitive data using emails disguised to look like trustworthy sources (Stavroulakis & Stamp, 2013).

The latest figures from the Anti-Phishing Working Group (APWG) for the 3rd quarter of 2017 show that reports of phishing attacks are increasing by approximately 10% quarter on quarter with over two hundred and ninetysix thousand received for the period. The report also states that attackers are becoming increasingly clever, using tools such as stolen certificates and spoofed secure URLs to trick targets, perhaps in response to better automated detection tools and more experienced users (Anti-Phishing Working Group, 2017).

Even as users become more aware of phishing attacks and detection technology improves, this attack vector continues to prove effective for attackers. While exact figures are impossible to know, due to the sensitivity of the issue, certain high profile incidents from the past few years could have only been perpetrated through the use of phishing. The much-reported rise of ransomware, including the "Wannacry" attack that famously took down the UK's National Health Service for a period in 2017, and others such as "Bad Rabbit" and "Notpetya" are just three examples (Ehrenfeld, 2017; Jasper, 2017).

While automated tools are increasingly used to prevent phishing, their effectiveness is relatively poor. Instead, it is often down to the individual to recognise when an email is not legitimate (Alghamdi, 2017). This creates a unique problem because the way in which individuals process information can vary significantly based on many factors, including the user's level of education, computer literacy, occupation, experience and attitudes to privacy (Vishwanath, Herath, Chen, Wang, & Rao, 2011).

Several studies have investigated the best methods through which to educate end users about phishing (Alghamdi, 2017; Arachchilage & Love, 2014), however little has been done to differentiate between the subjects themselves.

Phishing is a form of social engineering and it can be a complicated subject. Existing studies have focused on elements as far reaching as demographics (Alseadoon, Chan, Foo, & Gonzales Nieto, 2012), (Sheng, Holbrook, Kumaraguru, Cranor, & Downs, 2010) (Tembe, Hong, Murphy-Hill, Mayhorn, & Kelley, 2013), type of user (Vue, Student, Schmidt, & Price, 2013), (Grabner-Kraeuter, 2002) and the context in which an attack occurs (Arachchilage & Love, 2014), (Dhamija, Tygar, & Hearst, 2006). Some interesting work has also been carried out on how user attitudes to privacy online or how they process information online (Parsons,

McCormac, Pattinson, Butavicius, & Jerram, 2013) can be shown to predict their susceptibility to phishing attacks. In addition, user experience has also been shown to trump technical knowledge when accurately identifying phishing attempts in some cases (Wright & Marett, 2010).

1.1.1. A Brief History of The Internet

The technical origins of the Internet can be traced back to the 1950s when the first concepts of wide area computer networking were first formed in research facilities in The United States, UK, and France. By the 1960s, the American government had funded the ARPANET project with the first message sent over the network in 1969 (Kim, 2005).

The first "social" interaction recorded via networking is widely accredited to some memos written by J.C.R. Licklider of MIT in August 1962 discussing his "Galactic Network" concept. Licklider predicted an interconnected set of computers, on a scale hitherto unimagined, through which everyone could quickly access information. While this was a very primitive network, it operated in the same basic way that the Internet does today. (Leiner et al., 2009)

By the 1970s, the internet protocol suite (TCP/IP) had been developed, becoming the standard networking protocol for ARPANET. By the 1980s, several national supercomputing centres had been established in universities around the world. In 1986 the NSFNET project would provide interconnectivity between these sites and the established supercomputing sites located in research and education centres in the United States (Leiner et al., 2009).

At the same time, Tim Berners-Lee, often referred to as the "Father of the Internet," was working as a computer science researcher at CERN in Switzerland. His development of a system to link documents and other resources into an information system accessible from any node on a network resulted in what would come to be known as "the World Wide Web". The World Wide Web consisted of an information space where content is accessed by distinct addresses or Uniform Resource Locators (URLs), interlinked with each other and labeled using hypertext links (Berners-Lee & Fischetti, 2001).

Hypertext links are displayed on a computer in a human-readable format and reference other locations of information that the user can immediately access, usually through the simple click of a mouse (Wardrip-Fruin, 2004). This simplicity of use meant that Internet use would no longer be restricted to computer scientists and could be enjoyed, instead, by the average user (Berners-Lee, Hendler, & Lassila, 2001).

By the end of the decade, commercial Internet service providers (ISPs) had been established, ARPANET had been decommissioned, and several private networks had been established in American cities. The last restriction on using the Internet to carry commercial traffic was

removed in 1995 when NSFNET was itself decommissioned, paving the way for the public Internet (Salus, 1995).

There were few indicators in the early days of the public Internet of the enormous social and economic changes that the Internet would have on the world. In the early 1990s, mobile phones were used almost exclusively for business and were expensive (Katz, Rice, & Aspden, 2001). Most households did not have computers and data transfer rates across the most commonly available dial-up networks were slow (Kim, 2005).

Internet adoption would slowly increase throughout the 1990s and into the 2000s, with advances in technology bringing personal computing devices into more users' hands. Electronic mail (email), initially used for business purposes, soon became popular with private individuals as a more efficient alternative to the postal service. Online forums, bulletin boards, personal websites, and blogs became popular as did early online e-commerce sites such as Amazon, established in 1994, and eBay, launched in 1995 (Ariguzo, Mallach, & White, 2006)

By the turn of the century, mobile data and greater access to computing in general, would see more people online and more services available for them to use (Kim, 2005). The phenomenon of social media, first experienced by many with the launch of MySpace in 2003 but in many ways brought to the masses by Facebook the following year, would eventually create a new level of social interconnectivity, ultimately blurring the lines between the physical and digital world (Gerbaudo, 2018).

When Apple launched its iPhone in 2007, it marked the convergence of faster and more available data networking and a genuinely intuitive mobile computing experience for users (Mace, 2010). Google's Android operating system followed in 2008 bringing the smartphone to a wider audience (Chin, Porter, Kate, & Wagner, 2011), paving the way for todays always on, always connected, digital society.

1.1.2. Online Fraud and Phishing

Fraud can be defined as the act of deceiving others for personal gain. Usually, fraud is perpetrated for monetary gain, however other motivations can exist such as personal prestige, political motivation or self-preservation (Becker, Volinsky, & Wilks, 2010).

It is an inseparable part of the human condition and a timeless concept (Found, 2015). Fraud can manifest itself in many ways, representing a wide range of injustices perpetrated by dishonest individuals. Some examples include forgery, confidence schemes, plagiarism, and with the advent of today's digital society, online scams perpetrated through bogus websites and phoney emails (Becker et al., 2010).

Email has become a particularly popular attack vector for fraudsters because, while practically every adult in the First World has and uses email for either business and/or personal purposes, they are often not well educated in how the technology works or how email can be used to deceive them (Sheng, Broderick, & Koranda, 2015). While the technological advances of the last decades have made the Internet available to many, the veneer of usability presented by modern interfaces masks a still complex technology that can be exploited by bad actors to compromise unsuspecting users.

Fraudulent attacks perpetrated by email are known as "phishing", a term coined in 1996 by hackers stealing America On-Line accounts by scamming passwords from unsuspecting users, and stemming from the analogy of using email "lures" to "fish" for personal information from a sea of Internet users (Dhamija, Tygar, & Hearst, 2006). Phishing is a type of social engineering attack in which attackers use spoofed emails to trick people into sharing sensitive information or installing malware on their computers. Phishing works because it avoids directly targeting the often secure systems people use, instead, targeting the user themselves.

Phishing attacks generally operate in three phases.

- Firstly, potential victims are identified and receive the spoof email.
- Next, the victim acts on the malicious instruction or activates the malicious content of the email.
- Finally, the attacker leverages the stolen information, usually for monetary gain (Hong, 2012).

Phishing has become a catch-all term for fraud using email. However there are several different types of phishing attacks, and perpetrators will often combine elements of each in an attempt to trick their victims (Chandrasekaran, Narayanan, & Upadhyaya, n.d.).

1.1.2.1. Spear Phishing

A spear phishing attack targets the end user in a specific way. Attackers will often gather intelligence about the individual and craft the spoof email to deceive them based on personal details or circumstances. Spear phishing is usually motivated by financial gain, and individuals who control money or information in organisations are often targeted in this sort of attack (Stavroulakis & Stamp, 2013). Targeting very high-value targets in this way, such as company CEOs, is often referred to as "whaling" (Banu & Banu, 2013).

1.1.2.2. Clone Phishing

Clone phishing refers to a type of attack where a legitimate and previously delivered email containing an attachment or link has its content copied and manipulated to create a visually

similar email. In this sort of attack, legitimate links or attachments are replaced with malicious content then sent from an email address disguised to appear legitimate (Banu & Banu, 2013).

This technique exploits the end users' trust in the legitimate sender and is often used to deliver malware or to direct the victim to a spoofed website where they are tricked into divulging valuable information to the attacker.

1.1.2.3. Link Manipulation and Redirection

Most phishing attacks leverage some manner of technical deception designed to make a link or attachment in an email seem legitimate, disguising the true nature of the email's content (Stavroulakis & Stamp, 2013). One popular method is to make the text displayed for a link appear to be a reliable destination while the address behind the text links to a site controlled by the attacker. Another trick with URLs, known as IDN spoofing, can allow visually identical website addresses to terminate on different sites, often malicious and controlled, again, by the attacker (Dean, Felten, & Wallach, 1996). IDN spoofig and URL redirects are a common attack vector for phishing attackers and often use the identities of legitimate organisations as cover for their deceptions (Dean et al., 1996).

1.1.2.4. Social Engineering

The motive behind any phishing email is fraud, and fraud is perpetrated by tricking the victim into performing a task or providing information under false pretences. While every phishing email will have a technical element, they will invariably also contain certain well-defined situational context in an attempt to manipulate the user into doing what the attacker wants. This may be achieved by falsely invoking a sense of urgency, implying a level of threat, instilling a sense of concern or invoking a sense of opportunity or reward (Chandrasekaran et al., 2006). In each case, the attacker will often attempt to manipulate the target using emotions such as fear, curiosity or greed. These are all emotions which can short-circuit the targets cognitive reasoning and undermine their ability to assess the content of the email presented to them in a rational manner (Button, Nicholls, Kerr, & Owen, 2016).

1.2. Research Problem

The advent of the Internet and its now ubiquitous place in society, has lead to a paradigm shift in peoples lives. Now more than ever, the digital world and physical world coexist through technology that could only be dreamt of even twenty years ago, but which is now a regular part of peoples lives. While the allure of a digital society is obvious for the benefits it brings, it has the inevitable consequence of attracting criminals who would seek to use this technology for their dishonest means. Improvements in both the availability and usability of services continue

to attract users of differing abilities to these platforms, and while detection technology is also improving, the potential for fraud continues to increase.

Previous research has focused on who is most susceptible to phishing and why however much of it is inconclusive or contradictory to other studies in the same area. For example, Jagatic et al. (2005) found evidence that females below the age of 25 were statistically more vulnerable to phishing attacks while this finding was later contradicted by Parsons et al. (2013). Several studies have focused on user behaviour and attitudes to privacy online (Anderson, Vance, & Eargle, 2013; Chakraborty, Vishik, & Rao, 2013; Debatin, Lovejoy, Horn, & Hughes, 2009), and while these may offer more consistent indicators of vulnerability to phishing attacks, these studies have not linked these behaviors and attitudes back to demography.

To date, training methods used to educate users against phishing attacks have not considered the individual being trained. Attitudes and behaviours are not obvious in the same way that age, gender, computer literacy can be and no study has so far sought to link behaviour to user type in the context of susceptibility to phishing.

1.3. Research Objectives

The primary goal of this research is to assess if different types of users, defined by demographics (age, gender, education, occupation, etc.), computer literacy (experience online, social networks, etc.) and attitudes to personal privacy perform better at identifying phishing attacks.

The secondary objective is to assess how each respondent processes the visual clues in each test and if this correlates with their grouping. Testing is structured in such a manner as to assess if the respondent is focusing on the technical elements of the email or its content in the context of the scenarios provided with each test.

The hypothesis (H1) is that there is a statistically significant difference in the performance of different groups against phishing attacks. In addition, patterns of behaviour for each group will show a clear correlation between user type and how they assess risk online.

The null hypothesis (H0) is that there is no statistically significant difference between the defined groups regarding their effectiveness at detecting phishing scams. If the null hypothesis is found to be true, there may still be measurable differences in how each group assesses risk online. However, it may be of little statistical value without evidence that it influences their susceptibility to phishing.

1.4. Research Methodologies

Several primary and secondary methods of research were undertaken to complete this study. The first stage consisted of a comprehensive literature review. This research provides an overview

of the background and existing body of knowledge about online fraud and phishing in particular. It also informs the design of the questionnaire and test examples, highlighting the areas identified in previous studies as potential factors in phishing susceptibility.

Informed by the existing body of research as described in the literary review, the next phase of research involved primary investigative research in the form of an online survey and phishing test. This quantitive survey was designed to segment respondents based on the four indicators of phishing susceptibility - demographics, experience, attitude to privacy and computer self-efficacy, identified in previous studies as warranting further investigation. The phishing tests were derived from existing research regarding the various attack vectors in use by online scammers. The tests are designed to primarily understand how respondents, as segmented along the lines of demographics, experience, attitude to privacy and computer self-efficacy perform in different scenarios, and focus on either technical or content-based clues to their legitimacy or otherwise.

The secondary goal of testing is to establish if participants from different groups process these visual clues differently which may be evident by comparing their results across each type of test.

Finally, conclusions and inferences are drawn from the analysis of the statistics derived from the results of the survey and phishing tests as described above.

1.5. Scope and Limitations

While research for this study focuses primarily on cybercrime and specifically on email fraud or phishing, it also crosses the boundaries of several other disciplines including psychology, law, and information technology.

The study includes several limitations due, primarily to time constraints and the need to obtain a sizeable sample. For example, the delivery of the survey and test over social media produces a large sample, however, the sample is inevitably skewed towards regular computer users due to the online delivery method of the study. Also, distributing the survey and test via social media potentially skews the nature of the sample towards the author's own demographic, through the inevitable use of personal connections. This is somewhat mitigated through distribution via both personal and professional networks but is a factor nonetheless.

Finally, the methodology used to assess how respondents assess visual information is limited, however, time and resource constraints prohibited other methods of data collection.

1.6. Document Outline

The organisation of the dissertation is described in the section below.

Chapter 2 - Literature Review is a summary and critical analysis of the existing body of research concerning phishing and user susceptibility to these types of attacks. In particular, it focuses on the shortcomings of existing technical solutions and the people problem, a phenomenon where user behaviour can often work against technology designed to safeguard their security online. Demographic and behavioural indicators of susceptibility to phishing attacks are examined, as is research focusing on how users process information online, how this is linked to the concept of trust and how combined, these factors can be exploited by attackers.

Special attention is also paid to studies that examine the effectiveness of training users to recognise phishing attacks and those that look at computer literacy and online experience as key criteria.

Chapter 3 - Design and Methodology focuses on the experiment which exists in two parts:

- **Part 1** is the survey, and this section describes the design of the questionnaire including the decisions made with regards to what information should be collected and what questions needed to be asked to do so.
- **Part 2** concerns the phishing test element of the study, a series of ten evaluation questions where participants are presented with a screenshot of an email accompanied by a scenario and asked to judge the legitimacy of the email. This section describes how the examples were designed, explaining the methodology used to obtain the information required to address the research questions.

This chapter also discusses the data collection methodology and the tools used to host the study, distribute the study to respondents and how data was collected and analysed.

Chapter 4 - Implementation describes the data collection phase including information about response rates, data completeness and the distribution of data across the samples.

Chapter 5 – Results and Analysis details and interprets the results of the survey and phishing test. Analysis of the data is conducted in two parts:

- First, respondents performance is examined based on the factors identified through previous research as indicators of susceptibility to phishing attacks – Demographics, Experience, Attitude to Privacy and Computer Self-Efficacy. This information is used to address hypothesis (H1), that there is a statistically significant difference in the performance of different groups against phishing attacks.

- Next, the statistically significant findings from the initial test are investigated to address the secondary objective which is an assessment of how respondents from different groups process the visual clues in phishing emails.

The results of the study are discussed and compared to the findings of previous experiments outlined in the literature review, with any new findings highlighted.

Chapter 6 - Conclusions and Future Work provides an overview of the research project in its entirety, outlining how the study contributes to the general body of research within the area of Cyber Security and identifies areas for further investigation.

2. Literature Review and Related Work

2.1. Introduction

As this chapter will illustrate, a lot of research has been conducted which investigates what individuals may be more susceptible to phishing attacks and online fraud, and the possible reasons why. Studies have focused on various elements of demographics and behaviour, but findings have been largely inconclusive or contradictory.

It would be impossible to collate and review the existing body of work in its entirety so for this study; the research concentrates on understanding how technology and people intersect online attitudes towards privacy within the context of internet use, and the role that education and training play in protecting users online. The concept of email fraud is also examined with the typical elements of a phishing attack described and classified. In addition, the role of trust and how attackers manipulate it to deceive the victim is investigated, and some key predictors of susceptibility to phishing are explored.

2.2. Technology and the People Problem

While advances in technology and threat detection have made it safer than ever online, several studies have established technology alone is not sufficient to protect end users (Alghamdi, 2017) and completely prevent phishing (Stavroulakis & Stamp, 2013). One reason is that attackers have proven very adept at adapting their baiting techniques to fool even the newest of technologies (Vishwanath et al., 2011) employing sophisticated evasion techniques that fool detection technologies. For example, the use of images instead of text can make it harder for anti-Phishing software that searches for keywords or phrases to identify suspicious emails. Javascript commands can be used to alter the appearance of URLs, placing an image of a legitimate address over the false address or using bait and switch techniques that redirect traffic from hyperlinks in the background without the user's knowledge (Stavroulakis & Stamp, 2013).

Another factor preventing technology from providing complete protection against phishing is that in many studies, anti-phishing software proved unreliable, either taking too long to recognise new threats or producing false positives where no threat existed (Zhang, Egelman, Cranor, & Hong, 2006). In addition, research shows that the security mechanisms used to protect information online such as authorisation, authentication, and encryption, are difficult for most users to understand (Kelley, Hong, Mayhorn, & Murphy-Hill, 2012; Tembe, Hong, Murphy-Hill, Mayhorn, & Kelley, 2013) and many users simply do not trust security indicators (Sheng, Holbrook, Kumaraguru, Cranor, & Downs, 2010).

It should be noted too that security is rarely a major concern when the user is focused on the task at hand (Dhamija et al., 2006). Most users also seem unaware that restricting access to their data

does not adequately address the risk associated with the amount, quality and persistence of the data they provide (Dhamija et al., 2006). This information is often used to perfect the attack vector in a phishing attack to better lure the target in (Banu & Banu, 2013) and it is no coincidence that phishing attacks on social media appear to be far more successful with studies showing a more 40% success rate (Vishwanath et al., 2011). This is an issue because the trend is that information technology will increasingly be used to collect personal information about people with both beneficial and detrimental consequences (Dinev & Hart, 2006), so regardless of how good security technology gets, it is crucial to address the people problem (Kelley et al., 2012).

The people problem is a phenomenon that observes that users often exhibit dysfunctional behaviour when using technology that they encounter technology they deem to be interfering with what they want to do. This behaviour can include avoidance of the technology, ignoring the information it gives or in some extreme cases, outright sabotage (Dickson & Simmons, 1970). The people problem has been cited as a key challenge when implementing any security technology. In one study, measuring the effectiveness of in-browser security pop-ups, users failed to check the browser's security indicators consistently, and while they sometimes noticed suspicious indicators, they were either unable to interpret the security signals or rationalised ignoring them completely (Wu, Miller, & Garfinkel, 2006). This same study also showed that most respondents had little clue as to how sophisticated a phishing attack could be and were unaware of what practices should be employed to stay safe online. The people problem is one of the reasons that, while some users are aware of phishing scams, awareness alone does not appear to reduce their vulnerability to attack or provide a mechanism for protection against them (Sheng et al., 2010). The existence of the people problem means that the most important factor in securing computer systems must be focused on the end user (Alghamdi, 2017) and, as such, the education of the end user is essential.

It is not enough to simply warn the user about risks, but it should instead aim to increase their intuitive understanding of what might be genuine and what might be false in the digital world (Downs, Holbrook, & Cranor, 2007).

2.3. Attitudes to Privacy

Internet users have a habit of revealing important personal information to strangers while hoping that their information will be safe (Debatin et al., 2009). Studies have shown that attitudes to privacy vary wildly between users with 25% of participants in one study unconcerned about privacy and 50% only concerned when they deem the situation warrants it (Sheehan, 2002).

When asked about phishing, in particular, some participants in previous studies have shown an awareness of the phenomenon, but those studies also showed that this awareness did not make

them any less vulnerable (Sheng et al., 2010). Even in test conditions, where participants were aware that they were looking for phishing scams, significant numbers of participants would fail to accurately detect phishing emails (Dhamija et al., 2006).

Internet users will also trade privacy for gratification (Anandpara, Dingman, Jakobsson, Liu, & Roinestad, 2007) and there is a paradox between the reported concerns of users regarding their privacy and the behaviour they exhibit online about keeping that information secure (Gandy, 1993). The explanation for this is that users recognise that it is necessary to trade an element of privacy to participate in online activities such as social media or online consumer services (Sheehan, 2002). In extreme cases however, research has shown that users who have difficulty in regulating their use of social media platforms are more susceptible to phishing attacks, likely in part to an underlying disregard for personal privacy and characterised by a large number of online connections, many of whom are not known to them in real life (Vishwanath et al., 2011).

The conflicting findings of many studies have meant a clear understanding of peoples views on privacy has eluded researchers and this has impeded the development of a fully protective policy framework (Miltgen & Peyrat-Guillard, 2014). What is apparent, is that there is no significant difference between the gender or income of Internet users with regard to their attitudes to privacy online. However, those with higher levels of education appear to be more circumspect and wary online (Sheehan, 2002).

The attitudes of the old versus the young are a little less easy to define with some studies suggesting that younger Internet users simply do not expect the same levels of privacy online, the very concept having a fundamentally different meaning across the generations (Sheehan, 2002). Paradoxically, other studies have found that there is a clear desire for privacy among younger users even while they operate in a digital society designed to extract as much personal data from participants as possible (Hoofnagle, King, Li, & Turow, 2010) and that privacy holds a similar value for all users regardless of age (Debatin et al., 2009).

Ultimately, Internet users balance the risk of their privacy being compromised to achieve the goal of their online behaviour. User susceptibility to phishing occurs due to a perceived lack of vulnerability because they lack effective strategies to identify phishing activity, even when fully aware of the risks (Tembe et al., 2013).

2.4. Education & Training

With technology alone insufficient to protect users online, it is important that the user is educated about both the security risks that exist online and how to keep themselves safe (Alseadoon, Chan, Foo, & Gonzales Nieto, 2012; Tembe et al., 2013). Education alone, however, is not always effective although there is conflicting evidence in this area. One set of subjects who received training in how to identify a phishing email were significantly less susceptible to phishing attacks immediately after the training took place, however, the effects of the training quickly wore off, with subjects returning to their previous patterns of behaviour within only a few hours (Vishwanath et al., 2011). In contrast, another study measuring the effectiveness of the "PhishGuru" training system found that subjects who participated in the course performed significantly better than members of the control group who received no training with improvements evident 28 days after completing the training (Kumaraguru et al., 2009).

The ineffectiveness of user training can be seen in studies where participants were tested using simulated phishing attacks in the financial domain (Anandpara et al., 2007; Downs et al., 2007; Sheng et al., 2010). While overall performance in these studies showed respondents to be broadly more suspicious, likely due to the many high profile education campaigns undertaken by financial institutions over the past few years, it was demonstrated that the specific tools employed by many institutions to validate their customer communications were ineffective (Jansen & Leukfeldt, 2016). For example, many banks will feature the customer's bank account number or last 4 digits of their credit card when sending an email however in most cases, respondents did not recognise this detail or simple were not familiar enough with this personal information for it to provide an effective tool for validation (Dhamija et al., 2006).

Evidence also suggests that the type of training that some users receive can, in fact, make them more susceptible to certain forms of attack. For example, many younger users are exposed to educational programs that focus on staying safe online. However, these programs focus on personal safety from online predators and cyberbullying and rarely inform participants about information security and privacy (Hoofnagle et al., 2010).

While informing users of the risks of online behaviour is useful, effective training must arm users with strategies to accurately assess online content and focus on increasing their intuitive understanding (Downs et al., 2007). Research also suggests a need to adapt and personalise warnings, training and educational tools to cater for different types of users, in particular, those belonging to an older demographic (Association for Computing Machinery, Special Interest Group on Computer and Human Interaction, New Zealand Chapter, CHI 2017, & Annual CHI Conference on Human Factors in Computing Systems, 2016).

2.5. The Role of Trust

Trust is a psychological state that can be defined by an intention to accept a degree of vulnerability on the basis of positive expectations about the intentions or behaviour of another (Miltgen & Peyrat-Guillard, 2014).

For trust to exist, the situation must present the user with a degree of uncertainty, vulnerability and the possibility of avoiding risk-based a decision of judgment about the situational conditions (Blomqvist, 1997). In this way, trust is a way in which our brains respond to complexity and ambiguity, short-circuiting the decision making process to reduce the semantic load on the user (Kelley et al., 2012). Internet users are forced to make choices to surrender a degree of privacy in exchange for the ability to participate in online activities and do so because they perceive the risk of information disclosure to be worth it (Dinev & Hart, 2006). Trust is an important aspect of online user behaviour because, in almost all conditions, users have a challenge in assessing other's potential for harm (Friedman, Crowley, & West, 2011). Also, the online world can prove complex for users with a myriad of visual clues to process when assessing not only the validity of information but the content of that information itself. Even in scenarios when the user is aware that the interaction is not with an authorised agent of the trusted organisation, for instance when dealing with buyers or sellers through an online auction site, there is evidence that the perceived honesty, reliability and trustworthiness of the organisation are attributed to some degree to those using the service (Dinev & Hart, 2006). As a result, there is a proven tendency in internet users to judge the information that is presented to them online on the basis of "look and feel" (Sheng et al., 2010), often making assumptions about a web page or email based on their perceived reputation of the sender (Iuga et al., 2016).

This is the main reason that phishing attacks tend to mimic familiar and trusted organisations. In doing so, the attacker hopes that the end user's familiarity and trust of whom they perceive the sender to be, will undermine their critical assessment of the email and cause them to fall for the trap (Parsons et al., 2013). The use of familiar symbols associated with legitimacy makes the deception possible because their association with a trusted association validates not only the email, but also the scenario within which the user is making the trust-based decision to interact (Stavroulakis & Stamp, 2013). In addition, users will manage familiar risk more cautiously than unfamiliar risk. This means that users will consistently behave with caution when the risk is familiar and understood but will often display a disregard for the level of risk associated with unfamiliar situations (Tembe et al., 2013). As a result, trust will often play a more prevalent role when users are presented with unfamiliar scenarios from a previously trusted entity, making the spoofing of emails from well-known organisations a popular and effective method for attackers (Iuga et al., 2016; Rajivan & Gonzalez, 2018; Sheng et al., 2010)

Peoples disposition toward trust can vary, and those more willing to place their trust in others are more likely to do so blindly, without fully understanding the background information relating to the trustee (Vishwanath et al., 2011). There is also evidence that users from different cultures have a different concept of online privacy and what personal information is appropriate to share however there is little evidence that this has an impact on their susceptibility to phishing attacks (Banu & Banu, 2013).

Where trust is key is in regard to information processing about users who experience a high degree of cognitive load in an online environment, as this has been seen to correlate positively to phishing victimisation in users (Vishwanath et al., 2011). In simple terms, the more difficult a user finds it to understand the digital environment the more likely it is that they will fall back on trust as a decision-making tool. In turn, those more likely to trust blindly are more susceptible to attack.

While trust can be a difficult thing to measure, there are online behaviours that can betray the degree of trust a user places in their environment. Facebook, for example, is a platform where users trade a significant level of personal privacy in exchange for the perceived rewards associated with the service (Dhamija et al., 2006) and research has shown that habitual users of the service are more prone to social media-based phishing attacks and users with more friends more susceptible again (Blomqvist, 1997; Debatin et al., 2009). There is an argument that some of this susceptibility stems from users forming a ritualised pattern of usage which in turn has reduced their cognitive interaction with the platform (Vishwanath et al., 2011).

There is also evidence, however, that users with a large number of connections have more trust in a positive outcome when sharing personal information with strangers and a more naïve attitude to trust in general (Alqarni, Algarni, & Xu, 2016; Blomqvist, 1997; Debatin et al., 2009).

2.6. Why Phishing Works

Phishing attacks all have one thing in common – they are designed to manipulate the victim into doing what the attacker wants them to do without their knowledge. Usually, the goal is to trick the victim into revealing sensitive data either directly or through malicious links or downloads. For the deception to be successful, attackers employ a range of technical and psychological tricks to simultaneously coerce the victim while disguising the nature of the trap.

Email continues to be the platform of choice for perpetrators of these attacks mainly because of its widespread use and the ease with which emails can be spoofed. Most phishing attacks are carried out by sending emails, carefully disguised as genuine messages from legitimate organisations, to a large number of recipients (Chung, Park, Wang, Fulk, & McLaughlin, 2010).

2.6.1. Technical Deception

Phishing attacks work because of the attacker's ability to simulate the look and feel of genuine websites and emails, tricking the victim through the use of images, links, logos, and images of security indicators. These visual tricks are common, and the attackers are often so adept at replicating legitimate content to disguise their attacks that even experienced recipients are often fooled (Dhamija et al., 2006).

One such trick is known as “typejacking” and involves the substitution of genuine email addresses or URLs with ones that are controlled by the attacker but which bear a close resemblance to the original through the use of substituted or omitted characters (Wu et al., 2006). For example, replacing or omitting characters in the “AMAZON.COM” URL might not be detected by the casual user, e.g., “AMAZ0N.COM” (replacing the “o” with the number “0”) or “AMZON.COM” (omitting the second “A”). Attackers can also mask the true nature of active content in an email using an image depicting a trustworthy URL or file type to mask the malicious content underneath. For example, masking an executable file with an image of a genuine URL (Dhamija et al., 2006; Jansen & Leukfeldt, 2016). Images can also be used to mimic windows containing genuine content from a genuine web page, mimicking a browser window or dialogue box, to fool the user into disclosing information such as login credentials (Dhamija et al., 2006; Parsons, McCormac, Pattinson, Butavicius, & Jerram, 2013).

These methods are effective because of the way we process visual information with studies showing that, as humans, we do not accurately distinguish between similar images, especially when processing content. This is due to the eye-movement based memory effect where people pay less attention to images that they have previously viewed and is a key factor in the success of phishing attacks (Anderson et al., 2013). The effect can vary across different age groups. However, this is likely due to factors such as older users being less impulsive and generally less familiar with online environments in general (Iuga, Nurse, & Erola, 2016a).

2.6.2. Coercion

While most phishing attacks contain some technical deception, as described in the previous paragraphs, attackers also use coercive tactics to lure the victim into clicking on the link, downloading the file or providing the information the attacker is after (Stavroulakis & Stamp, 2013). Typically, an attacker will use a contrived situation or personal persuasion to increase the chances of their deception being successful (Parsons, McCormac, Butavicius, & Ferguson, 2010). They rely on the credibility phenomenon, a situation where the target believes that the email represents a valid two-way communication process between them and another legitimate party.

To make the email credible, attackers will often replicate the content, look and feel of legitimate messages (Eisend & Schuchert-güler, 2006; Wright & Marett, 2010). In sophisticated attacks, it can be difficult to tell the difference if logos and images are copied perfectly. Instead, the content or language used should act as a clue because attackers will always employ certain tactics to coerce their targets into the trap (Dhamija et al., 2006).

Phishing attackers also use tactics which attempt to elicit a reaction. The attacker does not want the email recipient to spend much time analysing the email so will create scenarios which take advantage of some our most basic instincts – fear, curiosity, and greed (Parsons et al., 2013; Wright & Marett, 2010).

Fear is an effective tool and often used by invoking a sense of authority within the sender (Jansen & Leukfeldt, 2016). Attackers will often create a scenario where the user is presented with a serious problem, for example, an alert that there might be suspicious behaviour on an online account. This will be paired with a threat that the service will be terminated if the issue is not put right immediately and invite the user to verify themselves through the provided link, which will likely lead to a fake version of the service in question under the control of the attacker (Wright & Marett, 2010). This sense of urgency, combined with the threat from authority is designed to instil a sense of panic in the user and short circuit their reasoning and make them click on the link and surrender their details without fully appraising the situation (Stavroulakis & Stamp, 2013).

Phishing emails often contain offers that are too good to be true, such as the now famous “419” (named after the telephone code in Nigeria where it originated) scam where the attacker poses as a wealthy foreigner who needs the target’s help to transfer vast sums of money. In return, the target is promised a portion of the wealth, but inevitably they fall victim to a financial scam which can ultimately cost the victim a lot of money (Stajano & Wilson, 2011). This type of scam relies on the target’s greed, and its ability to override rational thought. The user will suspend their disbelief or ignore obvious red flags because of their decision to grab the carrot the attacker is dangling in front of them (Dhamija et al., 2006)

Curiosity, while not often an attack vector in its own right, is often used to lure unsuspecting victims into phishing traps. Preying on the inquisitive nature of their targets, phishers will often create scenarios where a victim might find they idly click on a link or attachment to see what it contains (Iuga, Nurse, & Erola, 2016). Curiosity has been used to great effect in social media scams over the last number of years, where viral posts used to harvest personal data from unsuspecting users. While not in the same vein as traditional phishing, the Cambridge Analytica scandal which shed a light on how Facebook uses personal data revealed that many users were

compromised when they consented to take an online IQ test, giving the organisation access to a lot more of their data than they realised in the process (Clark, Adams, & Craven, 2018).

In all of these scenarios, the attacker is using tried and tested forms of persuasion and research has shown that three in particular, "authority," "reciprocity" and "scarcity," were by far the most effective (Chakraborty et al., 2013). The "high priority" email that threatens the withdrawal of services to the user engages authority response mechanisms that challenge the targets ability to question the scenario, instead, compelling them to comply with the attacker's demands (Stavroulakis & Stamp, 2013). Reciprocity occurs when one person does something for another, and in doing so instils a sense of debt in that person (Kelley et al., 2012; Rajivan & Gonzalez, 2018). Similarly, the psychological persuasion tool of scarcity is used to coerce users into the phisher's trap using the age-old phenomenon that people want what they cannot have (Kelley et al., 2012).

Users appear to respond to different persuasive techniques. All users respond to authority with effectiveness depending on the context of the email relative to the user. Reciprocity was found to be a more successful technique in older users while scarcity was more effective against younger people (Association for Computing Machinery et al., 2016; Chakraborty et al., 2013).

Research has shown that a better understanding of the internet environment leads to lower susceptibility to phishing however it was also shown that the same users are prone to false positives, where they find even genuine emails suspicious (Downs et al., 2007). This is an issue too because it means that genuine communications are often ignored, detracting from the overall user experience online.

Email users also employ bad strategies for verifying emails, focusing on particular elements, such as the content and not the sender address, or vice versa (Kelley et al., 2012; Stavroulakis & Stamp, 2013). Ultimately, these attacks are successful because the target trusts the sender and trust is a mechanism used in situations where people have to cope with uncertainty or ambiguity (Grabner-Kraeuter, 2002).

2.7. Predictors of Susceptibility

This section examines existing research regarding the factors that make individuals susceptible to phishing attacks. Indicators of susceptibility include basic demographic markers as well as attitudinal indicators and other factors such as computer literacy and experience online.

2.7.1. Demographics

There have been many studies that have investigated if demographic characteristics can be linked to susceptibility to phishing attacks with mixed and conflicting results – often within the same study.

While some research suggests that female subjects between the ages of 18 and 25 are more susceptible to phishing (Tembe et al., 2013), other studies have found that older women are more vulnerable to such attack (Association for Computing Machinery et al., 2016; Iuga et al., 2016). This is contradicted again by other studies that suggest that there is, in fact, no correlation between age and gender concerning susceptibility to phishing (Dhamija et al., 2006). More significant may be that age was negatively correlated with self-efficacy (Debatin et al., 2009), which is the belief that one has in themselves to succeed in a certain situation or their ability to complete a task (Rajivan & Gonzalez, 2018).

Individuals with employment experience performed better in some studies, likely down to increased levels of phishing awareness training (Parsons et al., 2013) however this is somewhat contradicted by studies that showed the individuals from poorer backgrounds displayed a general suspicion of everything online which in turn lead them to be marginally less susceptible (Alqarni et al., 2016; Sheng et al., 2015).

Educational background seems to play little part in predicting susceptibility to phishing with multiple studies citing no significant difference in performance between individuals with different levels of education (Banu & Banu, 2013; Downs et al., 2007; Iuga et al., 2016). One exception relates to individuals who had participated in technology or information systems studies who were, in fact, less successful in identifying fraudulent emails, suggesting that knowledge in this area could make the user complacent.

Demography alone might be an unreliable indicator of phishing susceptibility, however examining the findings of these studies in detail reveals underlying conditions that can sometimes be linked to demographics that might play a more important role. One such study found that men were more likely to correctly identify suspicious online content than women but only by a small margin. Women, too, were more likely to click on suspicious hyperlinks and more likely to give personal information to phishing websites however this difference was attributed to a higher level of technical training in male respondents and not an underlying psychological factor. The same study also found that younger respondents (18 -25) were again receptive to phishing attacks but also cited contributing factors such as less experience online, lower levels of education and training in conjunction with psychological factors such as a lower aversion to risk (Sheng et al., 2010)

2.7.2. Online Experience

Online experience is cited as a key factor in predicting user susceptibility to phishing. One of the main reasons why people are fooled by phishing emails is because their awareness of the risk is broadly conceptual and does not translate into an effective strategy to interrogate information online. Moreover, while subjects who could correctly define what phishing means

performed better than those unfamiliar with the concept, those who had experience with commonly spoofed scenarios performed better again (Arachchilage & Love, 2014; Tembe et al., 2013).

There are several areas where user experience matters. From a technical perspective, users who understand the basic technical and conceptual frameworks of how email and the internet in general works, have a greater capacity for identifying technical flaws in phishing emails (Kelley et al., 2012). Many fraudulent emails exploit the syntax of URLs, domain names, or forge email headers, which the receiver is far more likely to recognise as fraudulent if they possess a level of technical understanding. For example, recognising that "email@amazoncompany.com" is not a genuine URL for "amazon.com" and should, therefore, be regarded as suspicious (Dhamija et al., 2006).

On a conceptual level, users who have a familiarity with the service are less likely to fall victim to a phishing attack related to that service. Their patterns of use form an intuitive understanding of what to expect from the organisation and they are more likely to identify the coercive elements of a phishing attack as being out of the ordinary. Previous emails form a baseline from which users can assess the phishing email, and this experience was found to be a greater indicator of susceptibility than dispositional factors (Iuga et al., 2016; Wright & Marett, 2010).

General computer literacy was shown to increase user's ability to spot phishing emails (Iuga et al., 2016) and this might explain why older users are more prone to falling for online deception than younger users.

Younger users have grown up with the internet and access to computing devices across a range of formats (PC, smartphone, tablet) and this experience makes them better prepared to deal with privacy risks (Miltgen & Peyrat-Guillard, 2014), even if this can often be over-ruled by their more impulsive nature (Sheng et al., 2010). Older users did not grow up in a digital environment, and computer usage is a learned skill acquired by most at a later stage in life. As a result, older users tend to unknowingly share private information that can be misused by others (Chandrasekaran et al., 2006) and often fit the profile of the perfect phishing victim, combining low email usage or familiarity with a more submissive nature in the context of their behaviour online (Alseadoon et al., 2012).

2.7.3. Computer Self Efficacy (CSE)

Individuals are more likely to engage in a particular behaviour if they have confidence in their ability to effect a successful outcome. In an online environment, this means that users are more likely to participate if they are comfortable with their ability to understand and interact with the environment (Debatin et al., 2009). Self-efficacy, or confidence online is an important element

when assessing susceptibility to phishing attacks. Confidence and enticement beliefs are related to a willingness to disclose information online, and users with confidence in their abilities are more likely to resist the influence of phishing emails (Dinev & Hart, 2006).

Self-efficacy is indelibly linked to user experience, specifically, the amount of experience that a user has with communicating online with organisations or individuals, the scenario in which that communication occurs, the subject of that communication and, most importantly, the communication medium itself (Wright & Marett, 2010). Inexperienced users will generally exhibit a low level of self-confidence which makes them an easier target for fraudsters for several reasons. For example, email recipients with a low level of self-efficacy are typically accustomed to receiving help from others and are more likely to accept a provided solution without fully assessing or questioning it (Sheng et al., 2010; Wright & Marett, 2010). Also, experienced users should not only be able to detect subtle cues indicating deception in online environments, but their confidence bourne out of this experience makes them more likely to question any seemingly suspicious request, thus making them less susceptible to deception through phishing (Chakraborty et al., 2013; Iuga et al., 2016; Wright & Marett, 2010)

While subjects who expressed confidence in their ability to detect deception scored better, when tested, to those who expressed a lack of confidence in this ability (Kelley et al., 2012), there was also a discrepancy, especially among older subjects, between their self-reported susceptibility awareness and their behaviour during tests (Association for Computing Machinery et al., 2016; Chakraborty et al., 2013). This lack of self-awareness, or misplaced confidence, makes older users especially susceptible to phishing attacks (Chakraborty et al., 2013) but can also apply to individuals who believe themselves more capable than they are or who have become complacent online. Complacency has been identified as a trait amongst both younger users and those with a technical education (Downs et al., 2007; Wang, Li, & Rao, 2016; Wright & Marett, 2010).

2.7.4. Patterns of Use

Fundamentally, phishing scams are successful when the victim fails to successfully process the information that is presented to them (Vishwanath et al., 2011). Information is processed differently depending on the mental and physical capabilities of the user, so it is an important consideration when investigating phishing susceptibility (Sheng et al., 2010). The digital divide between old and young, as well as those who have access to services online and those that don't, has been cited as a reason why some users might lack the skills to defend themselves from online fraud. When studied, however, the breadth of the devide was not found to be as wide as originally thought (van Dijk & Hacker, 2003). While gaps in ability exist, other factors should be considered concerning susceptibility to phishing susceptibility (Parsons et al., 2013).

People use the internet for different reasons, and there is evidence that suggests that this too might influence user susceptibility to phishing attacks. Older users are more likely to search for health information, purchase goods or obtain information while younger users prefer to consume media, play games or read blogs (Debatin et al., 2009). Users of all age groups participate in online communities however older adults make up communities with distinct characteristics of behaviour online (Downs et al., 2007). They tend to be more interactive with other community members and more loyal to the community platform. This observation further supports the idea that older users have a more narrow area of expertise online making them more vulnerable to coercion that forces them outside of their comfort zone. While less of an issue, younger users display little loyalty for community platforms, often moving from one to another as fashion dictates. On the one hand, this leads to the dissemination of private data across multiple platforms but may also deter complacency and encourage vigilance among this group (Wang et al., 2016).

Studies have shown that older users tend to act less impulsively, often spending longer in evaluating a web page or email than younger users (Iuga et al., 2016) however the cognitive load experienced by an older user can be much higher due to unfamiliarity with the symbols and positive indicators of security that younger users intuitively recognise (Parsons et al., 2010).

Some suggest that the manner in which one navigates the world wide web mimics human memory and information processing (a construct known as isomorphism). In theory, this makes it superior to the traditional print media that older users would have grown up with. Others have argued that the sheer volume of information can lead to cognitive overload and disorientation for some users (Eveland & Dunwoody, 2001). As discussed previously, excessive cognitive load triggers comping mechanisms within the human brain causing users to fall back on decision-making mechanisms such as trust which can be easily exploited by attackers (Vishwanath et al., 2011).

2.8. Literature Review Summary

This chapter has explored a broad range of literature relating to online fraud and phishing attacks, focusing specifically on the phenomenon of phishing attacks via email.

The role of technology in protecting people from online fraud was examined, establishing that technology alone cannot be relied on to protect user's privacy. This is partly due to ineffective past implementations of these technologies but more importantly due to the user behaving in such a way as to undermine their effectiveness. It is well established that the user is often their own worst enemy concerning their online privacy, regularly sabotaging the controls put in place to protect them due to impatience, a lack of awareness of the risks involved or a general lack of faith in the technology itself. Internet users from different groups can have different expectations

of privacy online, and while younger users generally have a lower expectation of online privacy, they value it no less than the older user. It was noted that while older users value their privacy more, they tend to be less well equipped to safeguard it than younger users who have grown up with the Internet.

Ultimately, users become susceptible to deception when they fail to recognise their vulnerability and lack the strategies to manage risk. As such, education and training, which often focuses on simply making the user aware of the risks, is ineffective because just knowing about the risk does not protect the user. Instead, it is important to focus on building up an intuitive understanding of the elements that denote a genuine or suspicious email because focusing on one element, such as a traditional indicator like bad grammar, does not adequately equip the user to detect increasingly sophisticated phishing attacks.

Trust and its relationship with phishing victimisation was also discussed, finding that trust is a form of mental shortcut employed when the brain is under cognitive load or is otherwise operating in an ambiguous situation where no clear decision is evident. Internet users balance risk for reward when participating in online environments, and while the manner in which users trust can be difficult to measure, certain behaviours such as having a large number of social network connections can be indicators that the subject is prone to placing too much trust in others online and as such could potentially be an easier target for attackers. Phishing attackers exploit trust by mimicking genuine trust indicators such as logos from trusted organisations or accepted security flags, to dupe the user into believing that the fraudulent email is in fact from a legitimate sender, highjacking the goodwill built up between the parties during previous, genuine, interactions.

Next, how attackers construct phishing attacks were examined, finding that there are several ways that attackers can manipulate the look, feel and content of emails to deceive the victim. These elements can be classified as either technical deceptions, relying on deception through technical means, or coercive tricks, where the attacker manipulates the victim through a specific scenario. In most real world cases, a combination of both is evident.

Finally, predictors of phishing susceptibility were reviewed, examining the role that demographics play in susceptibility. The evidence in this area is often contradictory with some studies suggesting that gender, age, and education level are factors while other studies have found no statistical significance to any demographic value. The same research, however, points to other underlying factors which may provide more of an insight into who is more susceptible to phishing and it is clear that online experience and computer self-efficacy are both key indicators. Also, how users behave online, be it the services they use or the communities they participate in, can influence how vulnerable they are to attack.

2.9. Research Gaps

Previous studies have concentrated on testing individuals ability to discern phishing attacks from genuine emails or websites and little else. Very little research has been done to try and understand how different users might be assessing the information presented to them to decide if something is real or fake.

Several elements go into a modern phishing attack, some of which are technical deceptions while some simulate scenarios to entrap the victim or other, similar forms of coercion. No study has to date assessed which type of deception is more successful, either individually or in combination or sought to define what type of user is more or less susceptible to each form of attack. In addition, a lot of studies are historical, and with recent data breaches becoming big news, the typical user is more likely to have received some form of training around phishing detection and is likely more security conscious in general. As a result, there is a gap in research regarding general susceptibility in an environment of heightened security awareness, and no similar test has taken place during a time when phishing and online security and privacy are so topical. The effectiveness of phishing awareness training is also unclear, with contradictory results evident in the existing body of research.

Similarly, much research conducted on phishing attacks has concentrated on what makes an individual susceptible from the perspective of demographics alone. While some interesting work exists regarding these indicators, many of these studies' findings have been inconclusive, with the findings of some studies contradicting those of others. It remains unclear if any one group shows an inherent vulnerability to phishing based on their demographics. However, indications are that factors such as age and gender may be statistically significant and warrants further research.

Finally, research indicates that stronger predictors of susceptibility to phishing may be the subjects general online experience and, related to this, their self-efficacy or confidence in their abilities to safely participate in online activities, as well as psychological factors such as their attitude to privacy and degree of trust in online environments. This is an area that warrants further exploration.

2.10. Research Questions Defined

The goal of this study is to assess if certain individual characteristics make users more or less susceptible to phishing attacks. Where previous studies have simply segmented respondents based on demographic groups, this research attempts to explore the decision-making strategies that users employ when assessing the validity of an email.

In addition, the effectiveness of phishing awareness training will be examined as well as other factors such as the role that attitudes to privacy and computer self-efficacy play in predicting susceptibility to phishing attacks. The primary goal of the research, therefore, is first to assess if different types of users, defined by demographics (age, gender, education, occupation, etc.), computer literacy (experience online, social networks, etc.) and attitudes to personal privacy perform better at identifying phishing attacks.

The secondary objective is to assess how respondents process the visual clues in each test and how this relates to their success in distinguishing between genuine and fraudulent emails. Testing is structured in such a manner as to assess if the respondent is focusing on the technical elements of the email or its content in the context of the scenarios provided with each test. The goal is to understand if users from different groups exhibit a common pattern of behaviour in assessing each example email.

The **hypothesis (H1)** is that there is a statistically significant difference in the performance of different groups against phishing attacks. Also, patterns of behaviour for each group will show a clear correlation between user type and how they assess risk online.

The **null hypothesis (H0)** is that there is no statistically significant difference between the defined groups regarding their effectiveness at detecting phishing scams.

If the null hypothesis is found to be true, there may still be measurable differences in how each group assesses risk online however it may be of little statistical value without evidence that it influences their susceptibility to phishing.

3. Design and Methodology

3.1. Introduction

In the previous section, several gaps in research were identified, and a set of research questions were identified. Several options were considered when deciding how to best answer the research questions. While the demographic element of the study is simple to address using traditional survey methodologies, the question of how the respondent is assessing the information presented to them during a phishing attack is more challenging. Ideally, respondents would be assessed using tools that measured physical characteristics such as eye movement around the screen, mouse pointer position or time spent on each page. Although this would yield excellent information, the technology required to capture this data was not available as part of this research. An alternative approach was therefore devised that focused on the design of the phishing problems themselves.

By designing each problem to focus on a particular type of deception, technical or coercive, respondents success across the range of tests would indicate which types of deception were more successful, and this information could be used to investigate if patterns of success or failure were statistically significant for each group.

The focus from the outset was to design research that would engage with respondents as this would be crucial in obtaining a large sample pool and minimise abandonment and incomplete responses. As such, the entire demographic survey and phishing test were designed to take less than 10 minutes to complete with simple multiple choice answers, and deliberate avoidance of complex features such as Likert scales or freely typed responses.

The following section describes the design of the survey and phishing tests along with the methods employed to collect responses and analyse the data.

3.2. Part 1 –The Survey

The demographic survey portion of the research consists of ten questions. The anonymity of respondents was deemed important from the outset because anonymous respondents are likely to answer honestly and participate fully. Also, General Data Protection Legislation (GDPR) compliance is required if personally identifiable information is collected as part of the study and this could be a potential issue if the study were published elsewhere in the future or cited in other work. The survey aimed to collect demographic information about respondents which would allow them to be grouped into categories based on those previously identified as being significant about susceptibility to phishing – general demographics, attitudes to privacy, experience and computer self-efficacy.

3.2.1. General Demographics

Previous research has suggested that factors such as age, gender, education level and the area within which subjects work or study are the most relevant predictors of susceptibility to phishing attacks.

Questions 1 – 4 ask respondents to provide this information by selecting the range or category which most relates to them. For example, respondents are not asked for their specific age due to data privacy concerns and are instead asked to select the age range that applies to them. Education level covers a range of possible answers from no formal education, right the way up to Doctorate, including professional and trade qualifications. Area of work or study offers respondents a range of very broad categorisations to choose from, in an attempt to streamline the response process and reduce the effort required on the subject to complete the survey.

The goal of each question is to find out the following:

- ***Question 1:*** The approximate age of the respondent will determine if the subject falls into the older category where computer skills are acquired in later life or, the younger category of digital natives.
- ***Question 2:*** The gender of the respondent will be used to assess if there is a significant gender gap with regard to accurately identifying phishing attacks.
- ***Question 3:*** The respondents level of education will be used to determine if subjects with more or less formal education are susceptible to phishing and if those with vocational or professional training exhibit different patterns of response.
- ***Question 4:*** The area in which respondents work or study will be examined to assess how those working in different sectors perform relative to each other. Specific focus will be placed on those who work or study in business, finance or insurance as these individuals would have more contact with email on a day to day basis.

3.2.2. Experience

Evidence suggests that online experience, or lack thereof, may be a better indicator of susceptibility to phishing attacks than demographic information alone. Questions 5 – 9 ask respondents to provide information regarding their general IT and online experience along with an indication of their familiarity with the services used as examples in the phishing before performing those tests.

- ***Question 5:*** Respondents are asked to select from a list any services that they have used online in the past. The list includes categories for the real organisations spoofed (or otherwise) in the second part of the study to determine if previous experience with these types of services online makes the subject better at identifying phishing emails.

- ***Question 6:*** Social media usage is another indicator of online maturity. Respondents who have the largest number of accounts with the listed social media platforms are deemed to have more online experience than those with less social media presence. Note that the list of social networks used is not exhaustive but features the top 20 social networks as of January 2018.[1]

While not directly related to online experience, some inference may be made from respondents' answers to the following questions, although these are not intended as primary indicators in the context of this study.

- ***Question 7:*** While primarily intended as an indicator of privacy attitudes, this result will correlate with the previous question. Respondents with a large social media footprint who have met most of their connections in real life can be deemed to show a level of online maturity, validating, to an extent, the inferences from question 6
- ***Question 8:*** The respondent's self-assessment of their computer literacy is used to further assess experience with a focus on the technical aspects of online participation. The inference from these answers is that users who declare a high level of computer literacy should perform better at identifying technical deception.
- ***Question 9:*** Respondents who have received phishing training will have an enhanced level of experience versus those who have not been trained and will likely work in a role that requires the use of email for professional tasks. This would indicate a high level of experience. This question also relates to the somewhat inconclusive findings in previous research regarding the effectiveness of phishing awareness training in preparing users to avoid online deception.

3.2.3. Attitude to Privacy

In addition to measuring respondents' online experience, questions 6 – 7 provide insight into their expectations of online privacy. Using their social media footprint as a relative measure of how much personal information they have disclosed online, attitudes to trust can be inferred by how many of their connections are real-world acquaintances.

- ***Question 6:*** Respondents with a presence on a large number of platforms are assumed to have a medium to low expectation of privacy online due to the number of platforms across which their information is disseminated.

[1] Based on statistics retrieved from https://www.smartinsights.com/social-media-marketing/social-media-strategy/new-global-social-media-research/ excluding platforms not available in the EU and dating networks.

- ***Question 7:*** Respondents who state that they have met roughly half, or less than half, of their connections in real life will be categorised as having the lowest expectation to online privacy within the group of responders.

3.2.4. Computer Self Efficacy

Existing research cites computer self-efficacy as a predictor of success in identifying phishing attacks. Information from questions 8 – 10 will be used to assess the confidence that the respondent has in their ability to distinguish between the genuine and the spoof email examples successfully.

- ***Question 8:*** Respondents who rate their overall computer literacy will likely have greater self-confidence about identifying phishing emails.
- ***Question 9:*** Similarly, respondents who have previously undertaken phishing awareness training will be more confident in their ability to distinguish between genuine and suspicious emails
- ***Question 10:*** Respondents who declare that they expect to perform well in the test are deemed to have the highest computer self-efficacy rate. Part of the analysis will equate the answers to questions 8 and 9 with the assessment given in question 10.

3.2.5. Summary of Demographic Survey

The survey has been designed to gather information from respondents in four key areas that have been highlighted in previous studies as being significant as predictors of susceptibility to phishing attacks. These areas and the questions that relate to them are illustrated in Table 3-1 below:

<table>
<tr><th>Question #</th><th>Description</th><th colspan="2">Category</th></tr>
<tr><td>1</td><td>Age</td><td colspan="2" rowspan="4">A. Demographic Grouping</td></tr>
<tr><td>2</td><td>Gender</td></tr>
<tr><td>3</td><td>Highest level of education achieved</td></tr>
<tr><td>4</td><td>Area of work or study</td></tr>
<tr><td>5</td><td>Expereince with online services used in phishing tests</td><td rowspan="5">B. Experience</td><td></td></tr>
<tr><td>6</td><td>Social media usage</td><td rowspan="2">C. Attitude to Privacy</td></tr>
<tr><td>7</td><td>How many social media connects respondents have met in real life</td></tr>
<tr><td>8</td><td>Self-rating of computer literacy</td><td rowspan="3">D. Computer Self Efficacy</td></tr>
<tr><td>9</td><td>Has the respondent previously received phishing training</td></tr>
<tr><td>10</td><td>Self-rating on how successful the respondent expects to be in the test.</td></tr>
</table>

Table 3-1 - Survey Questions and How They Relate to Research Topics

3.3. Part 2 – The Test

The second part of the research requires participants to take part in a test to measure how effectively they can identify genuine or spoof emails. The goal is to measure the overall success of respondents and investigate if any groups, as defined in the previous section, perform better than others. The secondary goal of the test is to ascertain how respondents are evaluating the examples. The body of research has defined the technical and coercive deceptions that phishers often employ, and each test example has been designed to test one or more elements.

3.3.1. Elements of Testing

Test elements fall into two categories, technical and non-technical / content.

3.3.1.1. Technical Elements:

Sender Email Address: Many phishing attacks will mask the sender email address to make it look like it has originated from a legitimate source. The actual sender URL will often betray the true source of the email.

Bogus Link: One way in which phishing emails compromise recipients is by tricking them into clicking on bogus hyperlinks, often redirecting them to a website controlled by the attacker and designed to mimic a legitimate login screen through which the user's credentials are stolen

Bogus Attachment: similarly, another method of compromising the recipients of phishing emails is to disguise malware as a seemingly legitimate attachment or hyperlink

3.3.1.2. Coercive / Content Elements

Spelling / Grammar: Poor spelling and grammar have traditionally been clues that a phishing email is not legitimate. While phishing attacks have become more sophisticated, this is often still a feature of spoof emails.

Salutation: Most attackers will not have access to much of the data that legitimate senders do, such as the recipient's real name or other personal details. As such, many phishing emails will use generic or impersonal salutations which often provide a clue to the fraudulent nature of the email.

Contact Details Missing: Phishing attacks work when the recipient is successfully tricked into clicking on a bogus link, running malware or providing personal details in some other form. As such, phishing emails will often lack basic contact details for the spoofed organisation because the attacker will not want to risk the recipient contacting the organisation being spoofed and alerting them, or being alerted themselves, to the attack.

Sense of Urgency / Threat or Coercion: As discussed in the previous section, phishing attackers will often use the email to create a threat or sense of urgency as this elicits a response that often impairs rationality in the victim. As such, phishing attacks will often employ some ruse to coerce the victim into the phisher's trap.

Requests Personal Information: As the goal of most phishing attacks is to trick the recipient into sharing private information, phishing emails will often ask for personal information under false pretences. This is often a clue to the true nature of the email.

The example below in Figure 3-1 is one of the control examples which highlights most of the elements being tested for. Technical elements are highlighted in red, non-technical elements are highlighted in purple:

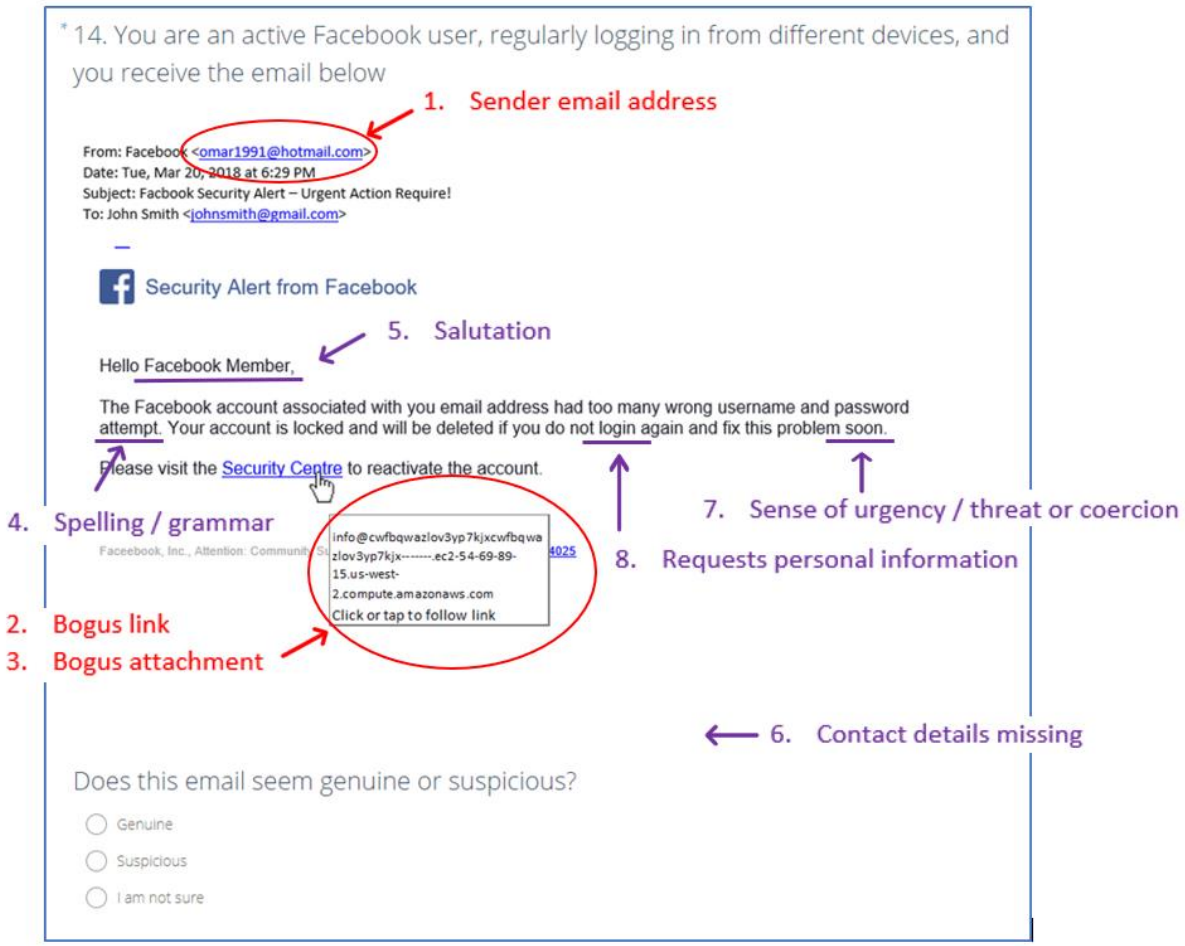


Figure 3-1 - Technical and Non-Technical Phishing Elements Illustrated

3.3.2. Designing the Test Examples

The email examples featured in the phishing test were designed specifically for this study. The decision not to reuse existing examples was taken for several reasons:

- Some recipients who had previously undertaken phishing awareness training may have had prior knowledge of some of the more common phishing email examples available online.
- The branding and look and feel of emails from large organisations changes all the time. Therefore it was important to use the most up to date examples to eliminate any cognitive bias that might arise from the use of older templates and logos.
- Existing examples, available from various sources, typically present the respondent with email tests presented through different email platforms. The experience of receiving an email on Outlook versus Gmail, for example, can vary. Using original mock-ups allowed for consistency across the test examples, especially in the area of header information.
- Mocking up the screenshots allowed important information to be included, such as the dialogue boxes presented when the mouse hovers over a link or attachment. It is impossible to simulate the respondent doing this themselves as part of this study, so the mock-ups include this information as part of the static screenshot.
- Lastly, the design of the overall test means that it is important that each test example has a distinct set of attributes which would have been impossible to achieve with existing examples. These elements are discussed in the next section

In total, respondents are asked to assess ten examples, seven of which are spoofed emails and three of which are genuine. The examples include four tests focusing on technical elements (one genuine, three fake), four tests focusing on content (one genuine, three fake) and two control examples (one genuine, one fake) which contain almost all of the elements in each case.

In each case, the respondent was presented with a scenario, the screenshot of the email and a simple question: “does this email seem suspicious?” The respondent can select one answer from three options:

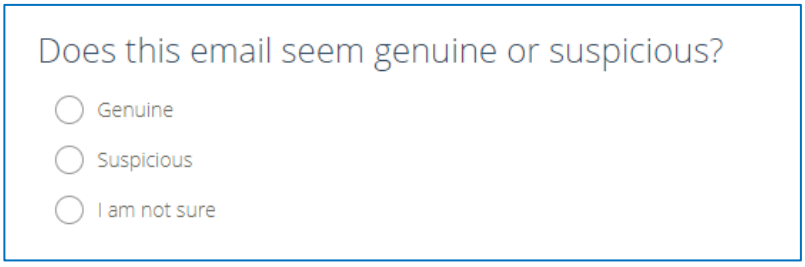


Figure 3-2 - Standard Multiple Choice Response to Phishing Tests

The “I am not sure” option is included so respondents are not forced to choose an answer when they are unsure. If this option was not present, it is likely that the results of the test would be negatively influenced by users guessing one way or the other. In the context of the overall test, where there is only one correct answer for each example, the “I am not sure” response is considered an incorrect answer.

3.3.3. Scenarios

In addition to the various technical and content related elements, each phishing example is accompanied by a scenario. Scenarios are included in an attempt to limit independent interpretation of the information presented in each case by definind a real-world context. Presenting email examples to respondents without context would undermine their ability to make an informed decision about the legitimacy of the email presented to them.

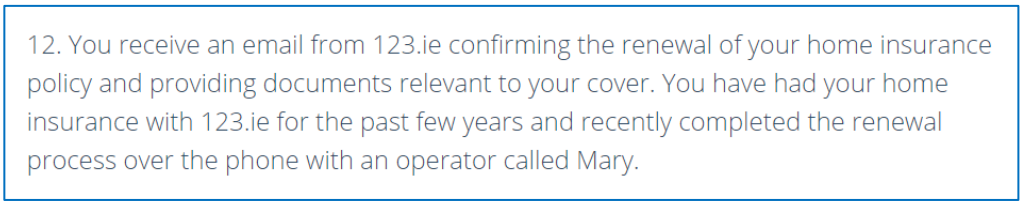


Figure 3-3 - Scenario Example From Phishing Test

The example above relates to the genuine control example where all elements of the email seem legitimate. The context of receiving the email might seem suspicious however if the respondent is not aware that, in this scenario, they have recently renewed their insurance with the organisation. It is, therefore, reasonable to expect to receive an email of the types used in this example.

The scenario tool is used in other examples to highlight the context within which the email has been received. Scenarios are designed to add legitimacy or suspicion to the email depending on the test.

The next section explains each phishing test, including the accompanying scenario and the test elements in each case.

3.3.4. Overview of the Phishing Examples.

3.3.4.1. Technical Phishing Example 1 - Microsoft OneDrive

Microsoft OneDrive is a cloud-based storage system included with Windows and available as an application on most operating systems that allows users to store and share photos, videos and other files[2]. The scenario and screenshot are presented as follows:

> *"You receive an email from your friend Aisling who you went to college with. Aisling wants to share some pictures with you from her recent trip to Spain using Microsoft OneDrive"*

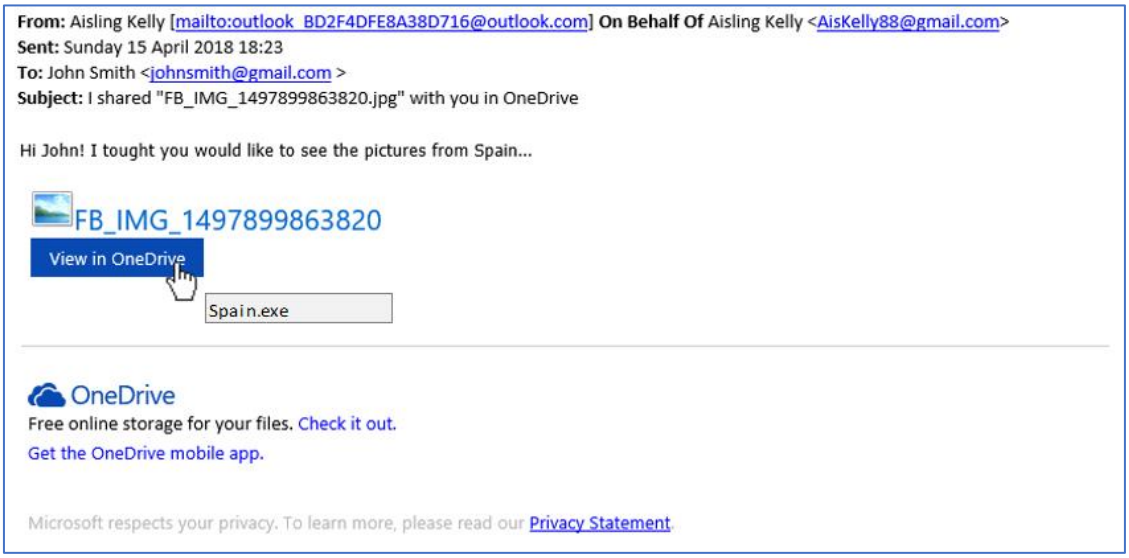


Figure 3-4 - Technical Phishing Test 1 – Microsoft OneDrive (Spoof)

The primary indicator in this instance is technical:

- **Bogus Attachment:** The indicator that the email is fraudulent is that the "View in OneDrive" link is itself disguising a file named "Spain.exe." While the name is plausible due to the content of the email, the user should not expect to receive an executable file. Photo sharing services always use either a link and/or a thumbnail of the photo being shared.

All of the other traditional technical indicators are correct, including the sender email address, as this is the format in which Microsoft send OneDrive link emails. Secondary elements are scarce because this is almost an exact copy of a genuine OneDrive email. There is some potentially coercion content depending on the mindset of the recipient. A woman sending

[2] https://www.microsoft.com/en-us/search/result.aspx?q=onedrive

pictures from a sun holiday may motivate male and female recipients to click on the link to view the pictures if for different reasons.

The scenario in this example is included to inform the respondent that "Aisling Kelly" is a genuine contact and AisKelly88@gmail.com is a genuine email address. This test is designed to mimic an attack where the sender's genuine credentials have been compromised, and the malicious file is being sent from their email address without their knowledge to existing contacts, unaware that their acquaintance has been hacked.

3.3.4.2. Technical Phishing Example 2 – Google / Google+

Google is the ubiquitous search engine, email provider, social media platform, operating system and just about everything else on the internet. Google places a strong emphasis on security and the third technical test exploits this[3]. The scenario and screenshot are presented as follows:

> *"Google is your email provider through their Gmail service and you also use your Google credentials on your Android phone, Google Maps, YouTube and several other websites. Your email address is "johnsmith@google.com" and you use a picture of Homer Simpson as your public profile pic on Google+"*

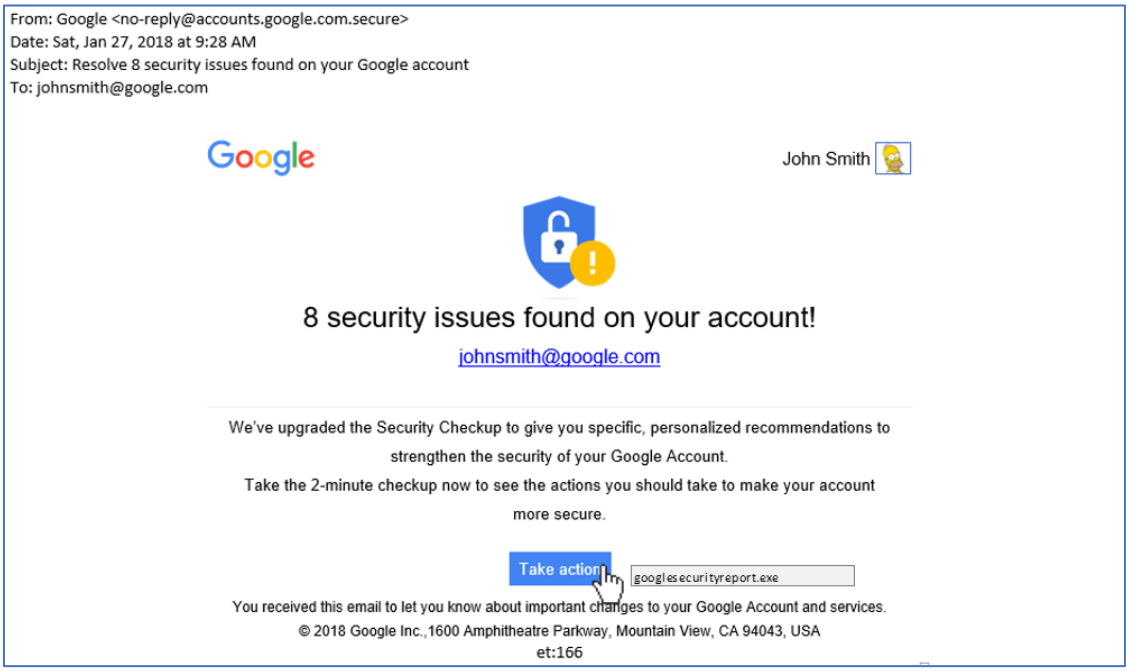


Figure 3-5 - Technical Phishing Test 2 – Google / Google+ (Spoof)

[3] https://www.google.com/about/

Based on a genuine Google security update email generated when a new device logs into the service, this test focuses on the following technical elements:

- **Sender email address:** while visually similar to a genuine google email address, the no-reply@accounts.google.com.secure sender address originates from a domain that does not belong to Google
- **Bogus link/attachment:** The other clue is that the "take action" button masks an executable file. This can be seen in the mouse over dialogue box which reveals a file named "googlesecurityreport.exe" where one would expect to find either a PDF, if indeed a report was attached, or a hyperlink if this was a genuine Google email.

In this example the context and content are interlinked. While the correct avatar and username lend an air of credibility to the email, the context refers to the fact that these items would be publicly available and easy to falsify.

Note that the avatar of Homer Simpson[4] is used to avoid publishing a picture of a real person. If a real photo was used in the fictitious user's avatar, it would be just as easy to copy it for this phishing email.

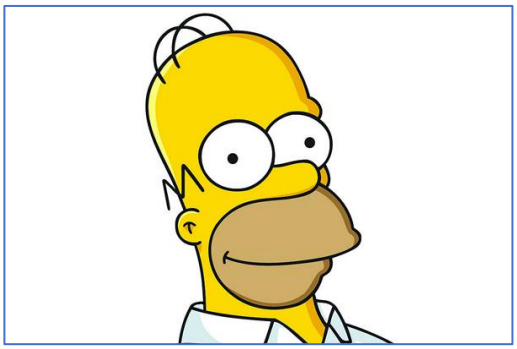


Figure 3-6 - Homer Simpson Avatar Image

This example also contains some limited coercive content. The alert that there are "8 security issues found on the account" is included to instil a sense of fear into the recipient in the hope that they will click on the link (in this case an executable file) without noticing the suspicious cues.

The example is intended to simulate a spear phishing attack where the attacker has conducted a degree of research on the victim before crafting the email. The use of the correct salutation and avatar lend legitimacy to the email, however, these are publically available items of information and easily replicated.

[4] http://interactive.nydailynews.com/2016/05/simpsons-quiz/img/simp1.jpg

3.3.4.3. Technical Phishing Example 3 – PayPal

PayPal is an online payments service, with over 192 million subscribers worldwide, that allows users to send or receive payment online from other users. It is the dominant platform in the online payments industry [5]. The scenario and screenshot are presented as follows:

> *"You receive an email from PayPal, who you use a lot to pay for things online. The email is a notification that you have paid a sum of money to a receiver you do not recognize or remember. This has happened in the past when the business name has been different from the trading name."*

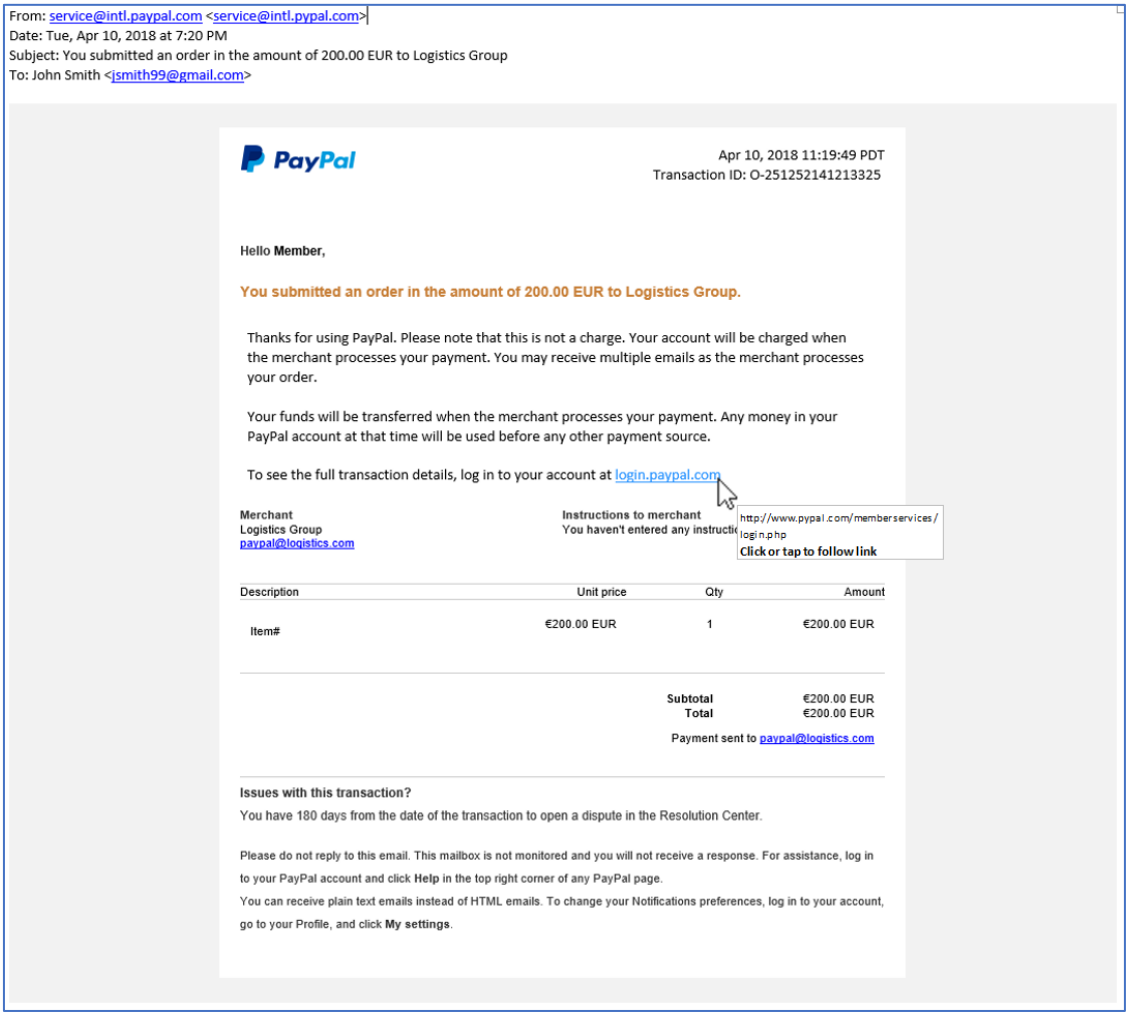


Figure 3-7 - Technical Phishing Test 3 – PayPal (Spoof)

This test focuses on the technical elements of the email. While there are some secondary clues in the content of the email, the primary indicators that this email is fraudulent are technical clues.

[5] https://www.paypal.com/ie/webapps/mpp/personal

This technical test comprises the following primary elements:

- **Sender Email Address:** the genuine PayPal email address of service@intl.paypal.com masks the real sender ID which is service@intl.pypal.com – note the missing "a" indicating that this is not a legitimate PayPal domain.
- **Bogus Link:** This same trick is used elsewhere in the email where the user is invited to log in to their account in the same "pypal.com" domain. Note the URL revealed in the mouse over dialogue box.

Although outside the scope of this test, clicking the link would redirect the user to a login page with a look and feel like a genuine PayPal login screen. If this were a genuine attack, this method would be used to steal the users Paypal login credentials.

There are secondary clues within the body of the email:

- **Salutation:** The salutation is a subtle clue because most professional organisation make it their policy to communicate with their members using their correct names.
- **Sense of urgency/threat or coercion:** there is a sense of urgency because the amount is large enough to worry the user they do not remember the transaction. In this case, the transaction never happened so it is likely the user would query it. The name of the fictional recipient is kept specifically vague to press the user further into clicking on the bogus link as is the 180-day time limit imposed to check the authenticity of the transaction.

The context of this email is presented to make the respondent aware that it is normal to receive emails from PayPal so that in itself is not suspicious. In addition, the context of the email is also used to direct the user to evaluate the email on its own merits and defocus on certain items that could act as a red herring, such as the fictitious "Logistics Group" is not an indicator of legitimacy or otherwise in the example.

3.3.4.4. Technical Phishing Example 4 – Parcel Motel

Parcel Motel is a sub-division of Nightline Couriers that provides a private PO box service for customers[6]. The scenario and screenshot are presented as follows:

> *"Getting goods shipped to Ireland can be a pain so you often use Parcel Motel, a courier forwarding service, to get cheap shipping from the UK. You receive the below email informing you that you have insufficient funds for your latest delivery which you suspect is that order you placed a few days ago."*

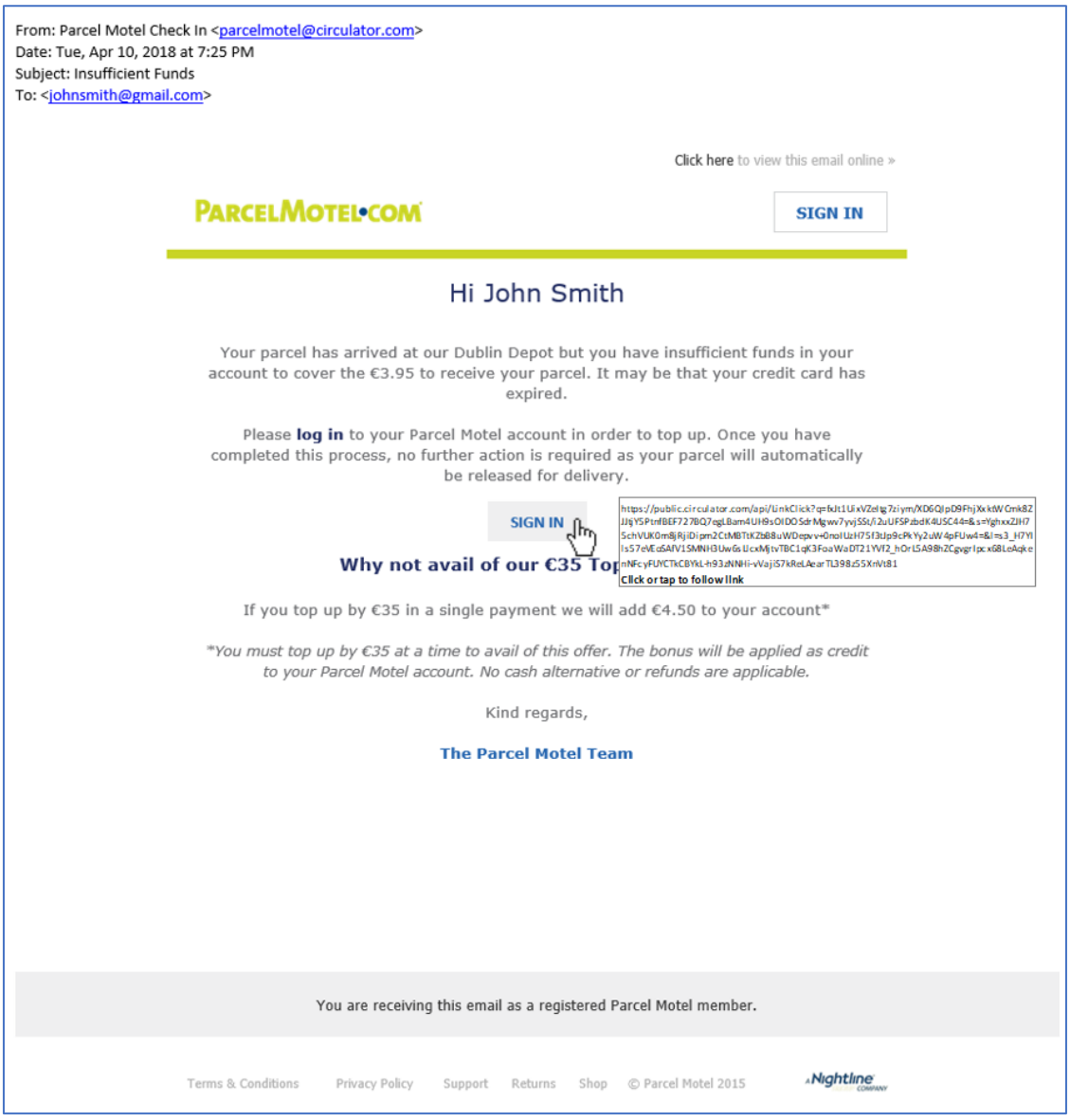


Figure 3-8 - Content Genuine Test - Parcel Motel (Genuine)

[6] http://www.parcelmotel.com/

This is an example of a genuine email where only the details of the recipient have been changed for privacy reasons. Unlike the previous test, this example displays all of the traits of a genuine email from a content perspective, however, many of the technical indicators could be deemed suspicious. From a non-technical perspective:

- **Spelling / Grammar:** spelling and grammar are all correct throughout the email
- **Salutation:** the email greets the recipient by their full, correct, name.
- **Contact Details Missing:** additional contact details are provided within the email through the "view this email online" hyperlink and the sign in button
- **Sense of urgency/threat or coercion:** the wording of the email simple informs the user of a problem in simple, neutral language.
- **Requests personal information:** there is no request for personal information.

The technical elements are somewhat at odds with the content, however:

- **Sender email address:** the sender email URL does not contain the Parcel Motel domain, instead originating from "circulator.com."
- **Bogus link:** similarly, the link provided directs to the same domain as evidenced by the mouse over dialogue box

Interesting to note is that "circulator.com" is registered to RackSpace[7], a data centre in the UK. This is a genuine email so it must be assumed that Parcel Motel host their email servers here and use the provider's domain.

The scenario provided in this instance suggests that the receipt of such an email would not be unexpected however the email is not explicitly validated.

[7] https://dawhois.com/?query=circulator.com; https://www.rackspace.com/en-gb

3.3.4.5. Content Phishing Example 1 – AIB Bank

AIB (Allied Irish Bank) is an Irish banking institution that offers customers a full online banking service[8]. The scenario and screenshot are presented as follows:

> *"Your bank (AIB) emails you to alert you to suspicious activity on you online banking facility. You have been an AIB customer for years and use the online banking facility regularly"*

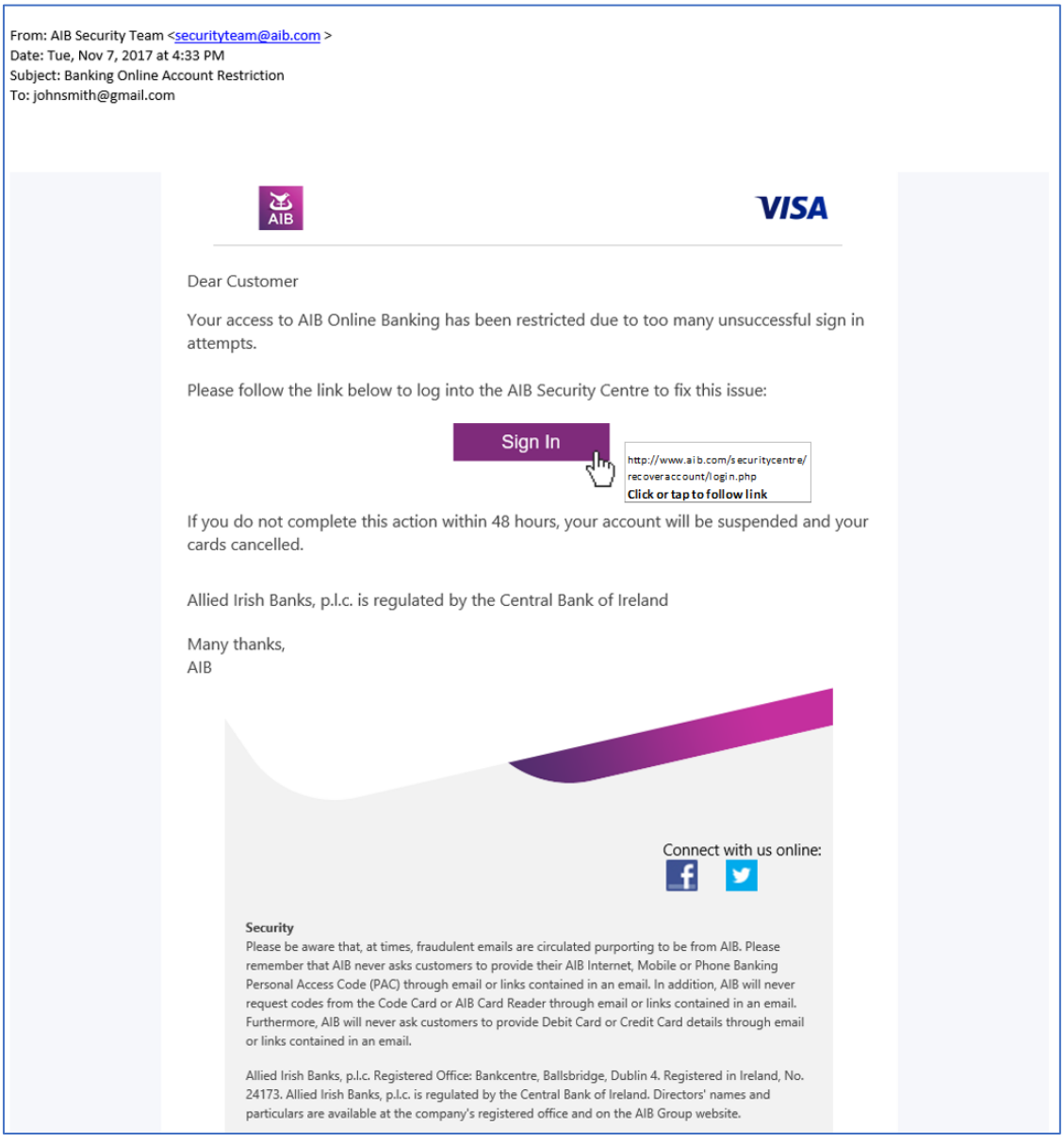


Figure 3-9 - Content Phishing Test 1 - AIB Bank (Spoof)

This example provides many clues to the fraudulent nature of the email. While the secondary clues are technical, the primary indicators are included in the content:

[8] https://aib.ie/ways-to-bank/internet-banking

- **Salutation:** the email addresses the recipient as “Dear Customer”. Most financial institutions include addressing their customers by name as a standard security practice, and AIB is no different. There is also no other information included, such as the last digits of an account or credit card number, to prove that the communication comes from a reliable source.
- **Contact details missing:** the email has been stripped of all of the usual contact details and URLs usually present in such emails.
- **Sense of urgency/threat or coercion:** the message contained within the email is designed to alarm the recipient and elicit a knee-jerk response. The message that access has been revoked to online banking due to “too many unsuccessful login attempts” is included to make the recipient think that they have been compromised. In addition, the threat of revoking all services if the situation is not rectified within 48 hours is included to hasten action on the part of the recipient.

In addition, the footer of the email, which was taken from a genuine AIB email, warns against fraudulent emails although not this kind specifically.

The secondary technical indicators are deliberately subtle:

- **Sender email address:** in this example, the sender email address, at first glance, appears genuine however AIB only use the “.ie” domain, and “aib.com” is not legitimate.
- **Bogus link:** while the link in the email seems genuine, “aib.com” is again, not a valid AIB domain. Like previous examples, this would lead to a spoofed login page if this was a real-world example.

For context, the respondent is instructed that they are a long-standing AIB customer and a regular user of online banking. This is included, so the receipt of the email is not deemed suspicious in its own right but also seeks to avoid introducing bias by adding additional information. This is a good example of a standard phishing scam often used to target victims to steal their banking credentials.

3.3.4.6. Content Phishing Example 2 – United Parcel Service

United Parcel Service (UPS) is a global freight and courier company who operate globally and specialise in international package delivery[9]. The scenario and screenshot are presented as follows:

> *"You buy a lot of goods online and regularly receive notifications of parcels being shipped to you. While you cannot remember this particular order, it's not unusual for you to receive these notifications and not remember the transaction."*

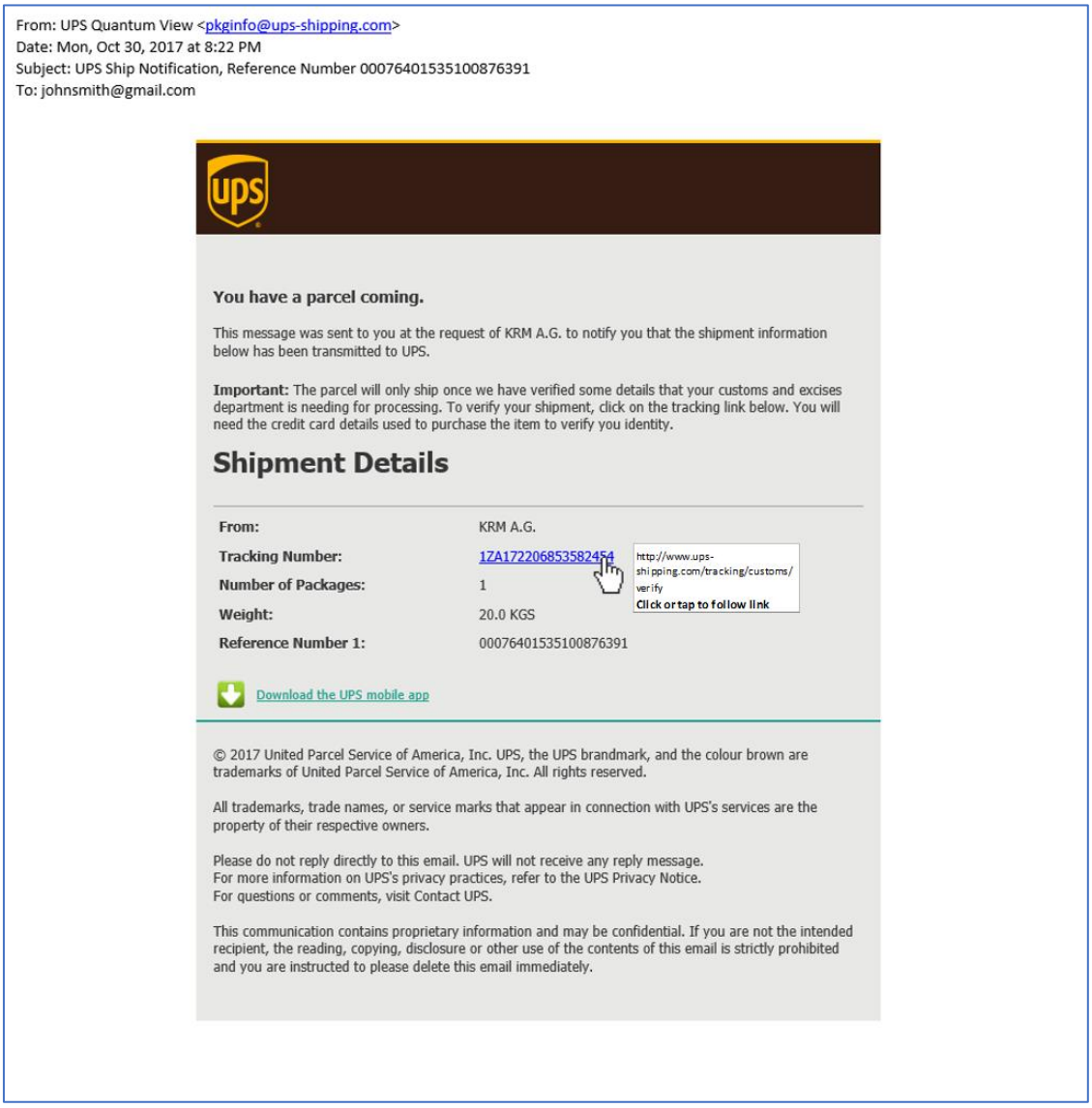


Figure 3-10 - Content Phishing Test 2 - United Parcel Service (Spoof)

[9] https://www.ups.com/us/en/about.page

This example again contains the primary indicators that it is fraudulent within the content of the email with some secondary evidence observable in the technical elements:

- **Spelling / Grammar:** there are numerous spelling and grammatical errors throughout the email. The subject line reads “UPS Ship Notification”, not “shipping” which would be more correct.

  The body of the email refers to “Customs and Excises” instead of “customs and excise”, “is needing” instead of “needs” and “you identity” instead of “your”. These clues indicate that email was written by someone to whom English is a second language.

  Note too that marketing departments from large multinationals rarely allow communications to go out with such obvious errors in spelling and grammar.
- **Salutation:** the email contains no salutation of any kind, however, this is somewhat of a neutral point because these sorts of messages often don’t contain a name because they receive their information from a third party, not the recipient.
- **Contact details missing:** the email has been stripped of all hyperlinks except the malicious one. Corporate emails, such as this one, always contain a myriad of links to other areas of the organisations however this email does not.
- **Sense of urgency/threat or coercion:** the sense of urgency and threat go hand in hand in this example, with the prospect of the (fictitious) parcel not shipping used to coerce the recipient into providing their credit card details. Also, the message that the request stems from an official body adds an air of authority to the email.
- **Requests personal information:** this example explicitly states that the recipient is expected to provide their credit card details to ensure their parcel ships. This is a particular red flag because, in this scenario, shipping would be the responsibility of the sender.

Secondary technical elements include the following:

- **Sender email address:** this example again contains a URL with a seemingly plausible but fraudulent sender email address. “ups-shipping.com” is not a valid UPS URL.
- **Bogus link:** similarly, the hyperlink contained within the email points to the same fake domain which would be under the control of the attacker were this a real phishing email.

For context, the respondent is told that it is not unusual to receive this sort of email, however, the direction is left intentionally ambiguous so as not to validate or invalidate the email and introduce bias unintentionally.

3.3.4.7. Content Phishing Example 3 – Amazon.co.uk

Amazon is an online retailer who operates across several regions using distinct URLs. For example, Amazon.co.uk represents their UK store while Amazon.de originates in Germany[10]. The scenario and screenshot are presented as follows:

> *"As an Amazon customer, you receive emails from them all the time with various offers and promotions or to inform you of changes to the site."*

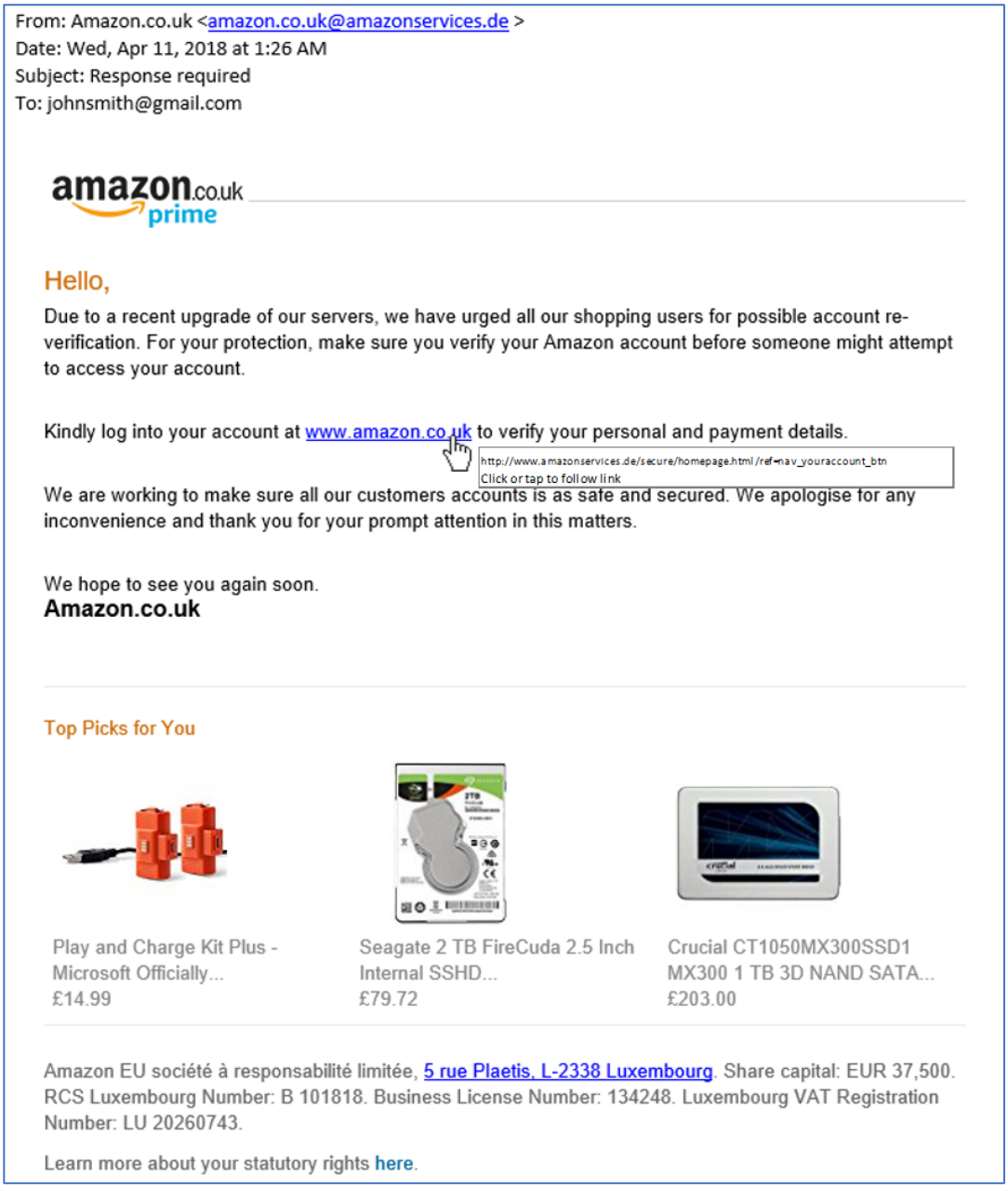


Figure 3-11 - Content Phishing Test 3 - Amazon.co.uk (Spoof)

[10] www.amazon.com, www.amazon.co.uk, www.amazon.de

In this example the primary indicators are found within the content of the email, however, some secondary technical indicators also exist. The primary indicators are as follows:

- **Spelling / Grammar**: the email includes numerous spelling and grammatical errors, for example: “we have urged all our shopping users for possible account re-verification”, “all our customers accounts is as safe and secured” and “your prompt attention in this matters.”
- **Contact details missing:** Amazon emails usually contain several additional links to other legal and promotional parts of their website. These are missing from this example as are other general contact details except for an address in the footer for an office in Luxembourg.
- **Sense of urgency/threat or coercion:** the threat is mild in this instance and somewhat implied. By disguising the email as an invitation to update personal details to ensure ongoing security, the email implies that failure to do so will leave the recipient vulnerable.
- **Requests Personal Information:** finally, the email states that the user should update their personal and payment details, informing the user that providing this information is what is required.

The secondary technical clues are deliberately subtle in this example so as not to overshadow the elements described above:

- **Sender email address: “**amazonservices.de” is not an Amazon email address and does not match the “amazon.co.uk” domain in the sender name.
- **Bogus Link:** similarly, the same URL is used in the bogus link which would direct the recipient to a fake login screen to steal their credential if this was a real phishing email.

The scenario provided in this instance informs the respondent that receiving emails from Amazon about a range of topics is normal.

3.3.4.8. Content Phishing Example 4 – Netflix (Genuine)

Netflix is the worlds most popular video streaming service, currently serving over 125 million users in over 190 countries[11]. The scenario and screenshot are presented as follows:

"Netflix, who you use regularly to stream movies and TV shows, emails you to inform you of some changes made to your account"

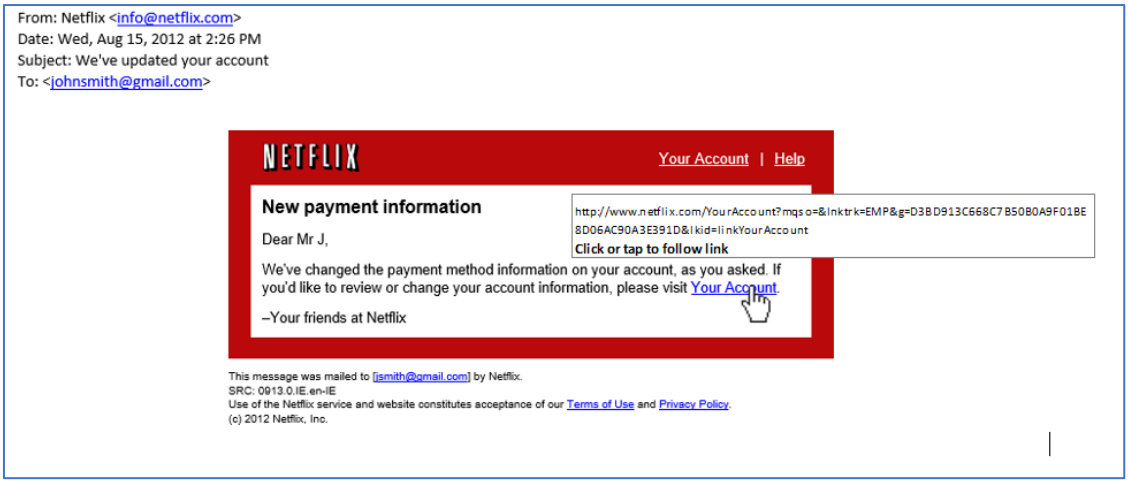


Figure 3-12 - Technical Genuine Test – Nextflix (Genuine)

This is an example of a genuine email with only the recipient's details changed for reasons of data privacy. From a technical perspective, all elements are present and correct:

- **Sender email address: "**info@netflix.com**"** is a genuine email from the Netflix domain which should not arouse suspicion.
- **Genuine link:** similarly, the mouse over dialogue reveals a link to a URL which is visibly part of the genuine "Netflix.com" domain.

This example is included because some elements could be misinterpreted as suspicious:

- **Salutation:** while present, the salutation of "Dear Mr J" seems suspicious even though this is genuinely how Netflix phrases its emails.
- **Sense of urgency/threat or coercion:** similarly, the email refers to a change in payment methods which could be a red flag
- **Other:** while the email provides some contact details, the 2012 copyright seems strange however this is a genuine Netflix email received within the last six months.

The accompanying scenario informs the respondent that they are a Netflix subscriber but does not add any additional context to avoid introducing bias on behalf of the respondent.

[11] https://media.netflix.com/en/about-netflix

3.3.4.9. Control Phishing Example 1 – Facebook.com

Facebook is a social media site that needs no introduction. With over 2.2 billion active subscribers[12] it is the most popular social network in the world. The scenario and screenshot are presented as follows:

> *"You are an active Facebook user, regularly logging in from different devices, and you receive the email below"*

Figure 3-13 - Control Phishing Test 1 - Facebook (Spoof)

This example of a phishing scam is intended to act as a control within the test, and as such, it includes many technical and content elements which should alert the respondent to its suspicious nature.

The technical elements are as follows:

- **Sender email address:** in this example, no attempt has been made to disguise the fact that the email has not originated from a genuine domain, the attacker using, in this case, a private email address omar1991@hotmail.com.

[12] https://zephoria.com/top-15-valuable-facebook-statistics/

- **Bogus link:** the hyperlink too is suspicious, linking to a site in the Amazon Cloud (AWS) as shown in the mouse over dialogue box.

In addition to the obvious technical clues, there are other clear indicators that the email is spoofed in the body of the text:

- **Spelling/grammar:** the email is littered with spelling mistakes and poor grammar. For example, “with you email address” and “too many wrong password attempt”.
- **Salutation:** the email addresses the recipient as “Facebook Member” instead of the recipient's real name. Facebook always use the subscriber’s proper name when communicating with them
- **Contact details missing:** the email is devoid of any additional contact information
- **Sense of urgency/threat or coercion:** the email falsely informs the recipient that their account has been locked and will be deleted if immediate action is not taken.
- **Requests Personal Information:** while personal information is not expressly requested, it is clear from the email that Facebook login credentials will be required to solve the issue.

The scenario presented to the respondent in this instance states that they are an active FaceBook user that accesses the platform from several devices. This is included to lend some level of plausibility to the fact that the respondent might receive such an email from Facebook without unduly biasing the respondent in any direction regarding the email’s legitimacy.

3.3.4.10. Control Genuine Example 2 – 123.ie

123.ie is the Irish online insurance arm of Royal Sun Alliance, an international insurer[13]. The scenario and screenshot are presented as follows:

> *"You receive an email from 123.ie confirming the renewal of your home insurance policy and providing documents relevant to your cover. You have had your home insurance with 123.ie for the past few years and recently completed the renewal process over the phone with an operator called Mary."*

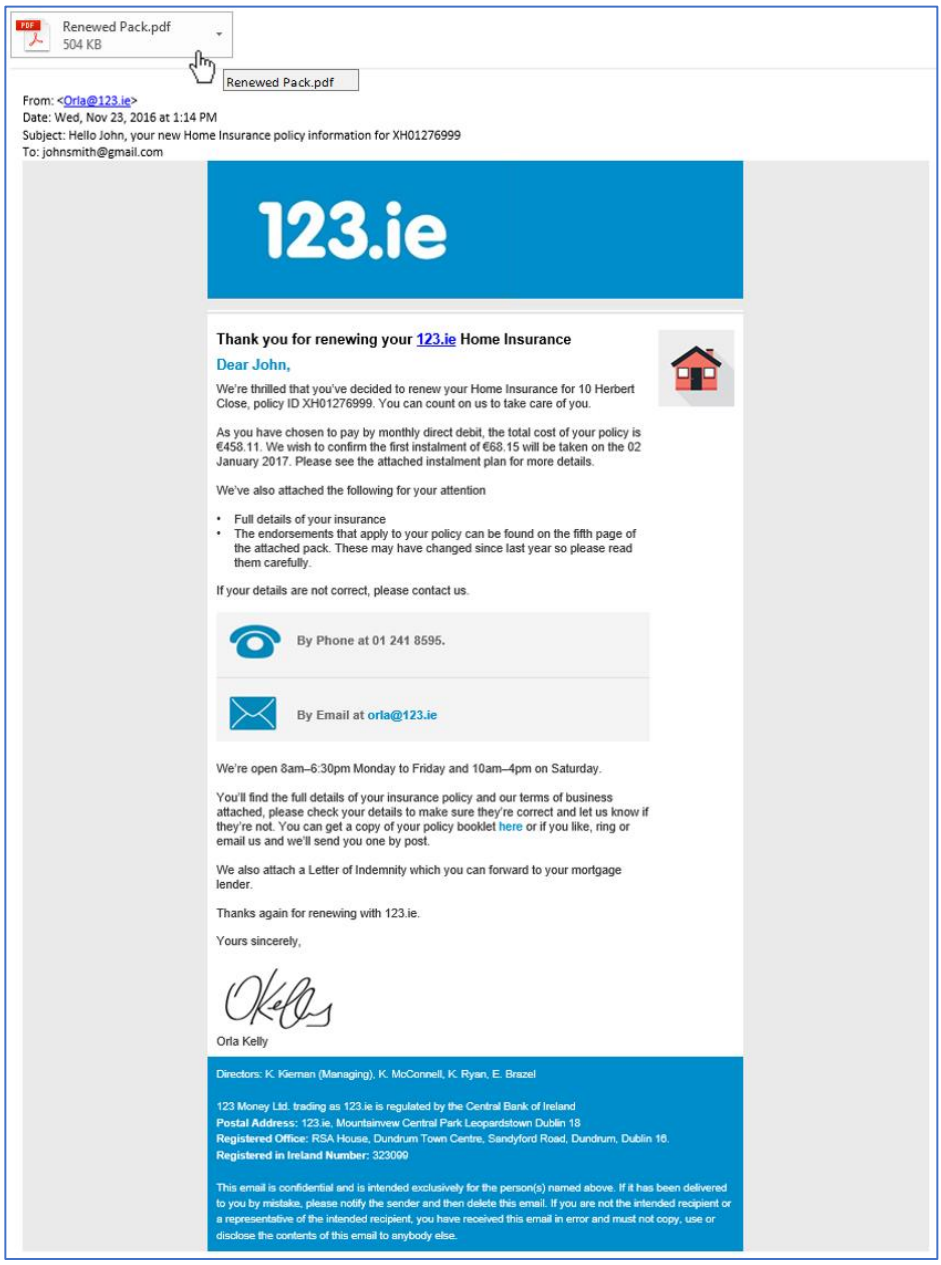


Figure 3-14 - Control Phishing Test 2 - 123.ie (Genuine)

[13] https://www.123.ie/about-us

This example is the second control test within the study and represents a genuine email that contains several technical and non-technical indicators that the email is legitimate.

The technical elements include:

- **Sender email address: "**orla@123.ie" originates from the 123.ie domain name
- **Genuine attachment:** the attached PDF claims to be details of an insurance renewal and the file name and type, as evidenced by the details contained in the mouse over dialogue box, support this.

The non-technical elements include the following:

- **Spelling/grammar:** the email written professionally using natural business language with no apparent spelling or grammatical errors
- **Salutation:** the email addresses the recipient as by their proper name and also includes a policy number that the recipient can check against their records. The latter is information that an attacker would be unlikely to have.
- **Contact details missing:** the email provides plenty of alternative ways of communicating with the sender including a telephone number. Alternative contact methods are usually absent from phishing emails because the attacker only wants the recipient to click on the bogus link or file.
- **Sense of urgency/threat or coercion:** there is no threat or sense of urgency or coercion evident within the email.
- **Requests Personal Information:** no request is made for personal information, the email instead offering the user details of their insurance policy as validation.

The scenario presented in this instance is designed to reinforce the legitimacy of this control example. The respondent is made aware that they recently renewed their insurance with the company and it is normal that a follow-up email would be received in such an instance. Adding that the customer service representative who handled the renewal was named "Mary" was included because all 123.ie communications come from the fictitious "Orla" which might raise suspicions in the most cautious and is a real-world scenario which the study wished to replicate.

3.3.5. Summary of Phishing Tests

The previous sections describe the ten simulated email examples designed to test respondents ability to identify fraudulent emails accurately. The examples are designed to test for the eight technical and non-technical elements based on existing research as detailed in the previous sections. Each phishing example contains one or more of the elements identified as shown in Table 3-2 below:

Descriptor	Test Name	Technical			Non-Technical				
		Sender Email Address	Bogus Link	Bogus Attachment	Spelling / Grammar	Salutation	Contact Details Missing	Sense or urgency / Threat or coercion	Requests Personal Information
Technical 1	OneDrive Photo Share	x		x					
Technical 2	Google account alert	x	x	x				x	
Technical 3	PayPal payment example	x	x			x		x	
Content 1	AIB account restriction	x	x			x	x	x	
Content 2	UPS shipping confirmation	x	x		x	x	x	x	x
Content 3	Amazon Account Verification	x	x		x	n/a	x	x	
Genuine 1	Netflix payment terms					x	x	x	
Genuine 2	Parcel Motel Insufficient Funds	x	x						
Control 1 (Phishing)	Facebook Security Alert	x	x		x	x	x	x	x
Control 2 (Genuine)	123.ie Home Insurance renewal								

Table 3-2 - Phishing Test Elements Matrix

The phishing examples were designed specifically for the study, using genuine and recent emails as a starting point. This allows for a level of uniformity across the test in areas such as the presentation of the email header and the simulation of the mouse over dialogue box, minimising bias that may have been introduced if a mix of formats been presented to the respondents. Using recent emails as examples means that the look and feel of each example is relevant and up to date, reducing any bias that might have occurred if older logos were used. The tests are purposely difficult in an attempt to simulate the real-world threat, however the testing apparatus, a simple presentation of a scenario, screenshot and multiple choice question, is deliberately lightweight to mimic the low cognitive load associated with normal email usage.

3.4. Data Collection Methodology

The best method of performing the research was identified as an online survey and test. Survey Monkey was selected as the online platform through which to perform the primary research for several reasons.

- Placing the survey online makes data collection easier, faster and more efficient.

- The anonymity afforded by an online survey reduces bias as respondents can answer questions without unintended influence from the tester.
- Survey Monkey provides a mechanism for distribution through social media and other digital channels and includes several additional tools to collate and analyse data. While these tools were not used in the analysis portion of this study, they proved useful by providing early indicators of data trends and interesting statistical results.

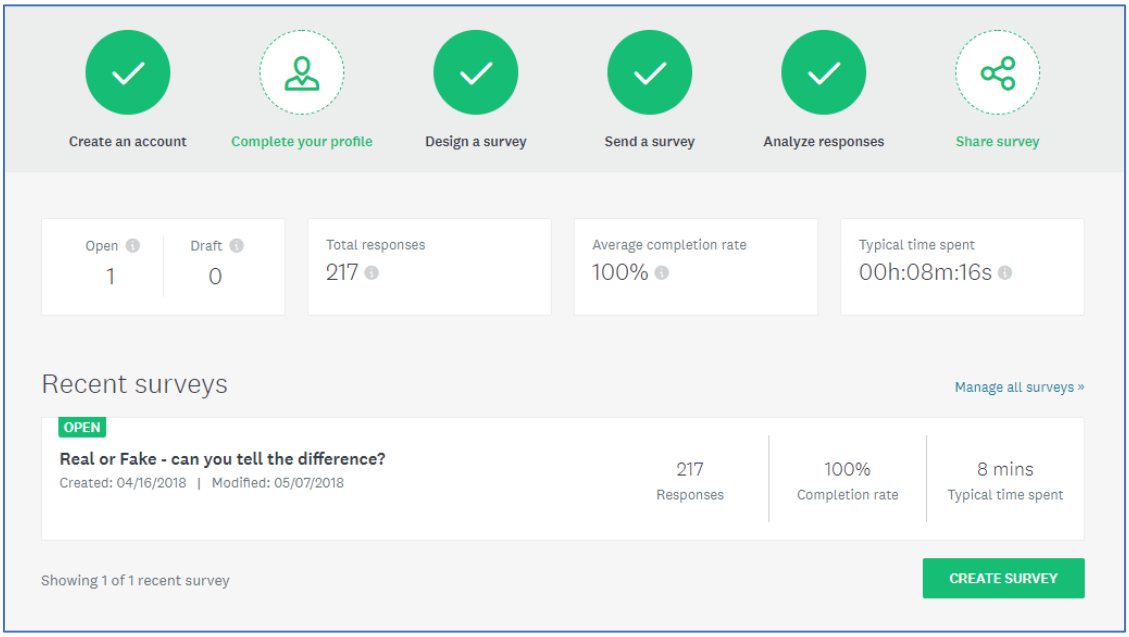


Figure 3-15 - Screenshot of Survey Monkey dashboard (post response cleaning)

The sample was selected using a process of convenience sampling, using Facebook and LinkedIn to distribute the survey and test. This approach was used to generate the greatest number of potential respondents while making the study as accessible as possible to a broad range of people who were not overly familiar with computer-related technologies or phishing in general.

The study was designed with this approach in mind from the outset in the hope that a compelling and low effort response requirement would encourage further dissemination beyond the initial distribution network. Using an online survey tool also allowed for better management of the sample respondents. Multiple responses from the same IP address were forbidden so respondents could not answer multiple times, enhancing the integrity of the collected data. Also, incomplete responses are flagged and were easily removed from sample data. In addition, Survey Monkey allows the survey to be built quickly at the outset, and data to be exported for further analysis once completed. The implementation and analysis of results are discussed in the following sections.

4. Implementation & Analysis of Sample

4.1. Introduction

The survey and test aimed to address the research questions as discussed previously. The main goal was to investigate if certain individual characteristics make users more or less susceptible to phishing attacks. The secondary objective was to assess how respondents from different groups process the visual clues in each test and if this relates to their success in distinguishing between genuine and fraudulent emails.

The study comprised of two elements – demographic information gathered about respondents through the questionnaire, and their actual performance across ten phishing tests designed to focus on common technical and non-technical indicators of spoof emails.

This chapter presents an overview of the study's findings, including a note about completion rates, an overview of responses and finally some in-depth analysis of the findings to address the research questions as described above.

4.2. Completion Rates

The survey was distributed through the tester's Facebook and LinkedIn networks, comprising of 256 and 1303 connections respectively.

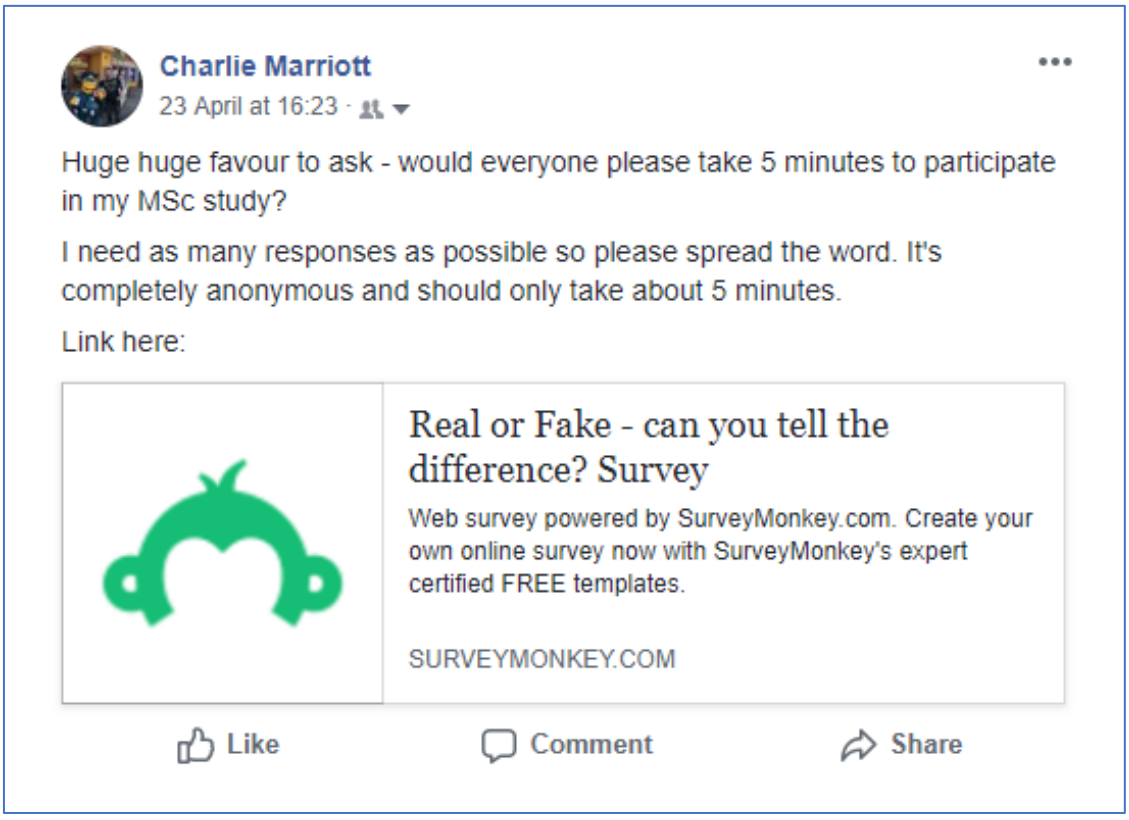


Figure 4-1 - Screenshot of Facebook Share

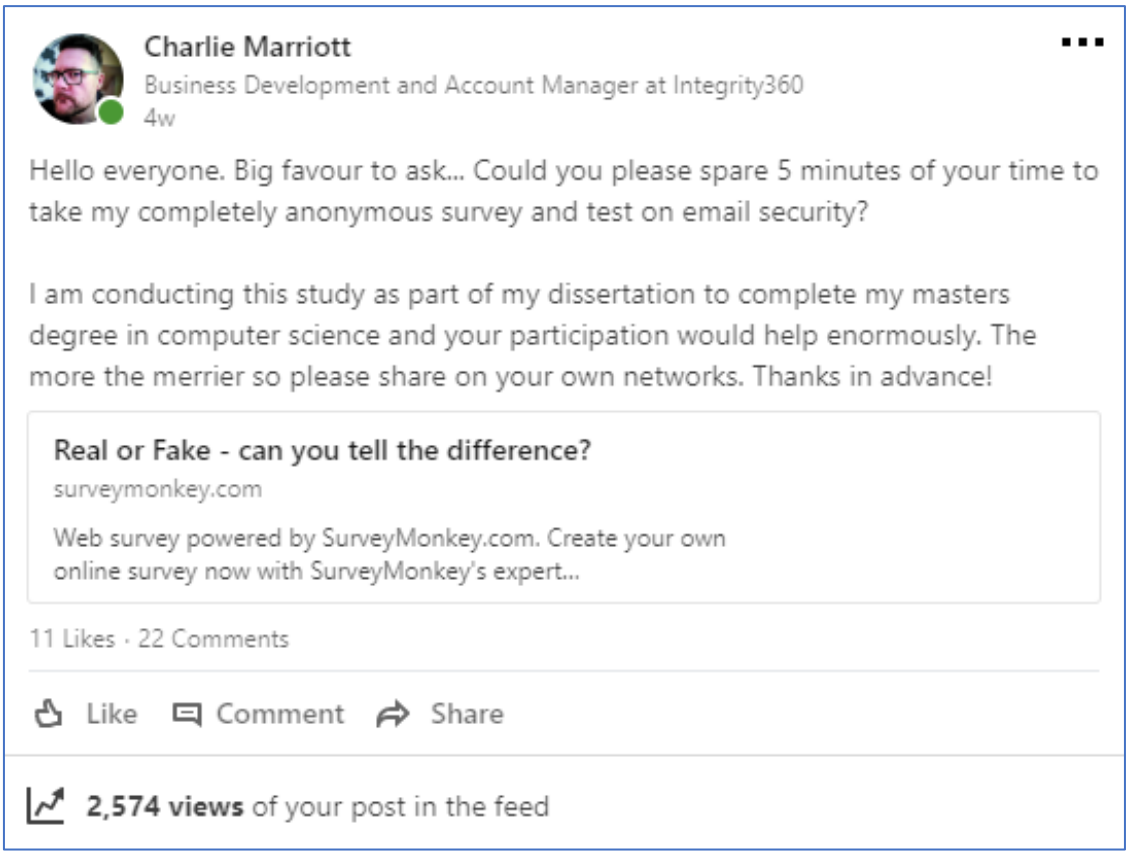


Figure 4-2 - Screenshot of LinkedIn Share

While analytics are not available for either platform, anecdotal evidence indicates that Facebook proved the most effective platform, providing roughly 60% – 70% of responses. This was due in part to respondents sharing the test within their social networks exposing it to a wider audience. The survey ran from 23.04.2018 – 07.05.2018 with the majority of responses collected in the first few days as shown below:

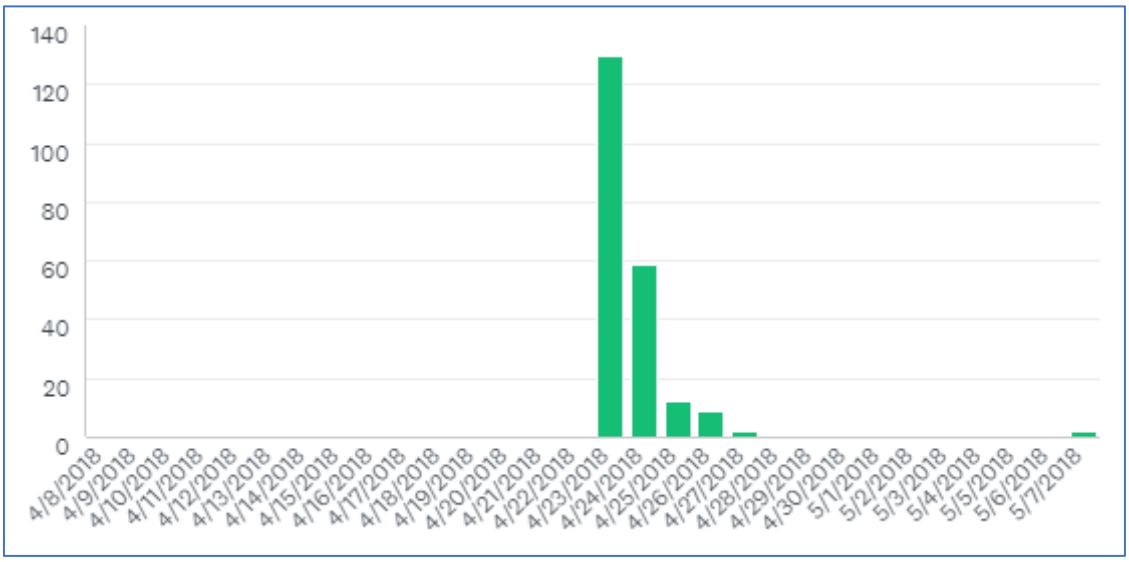


Figure 4-3 - Survey Response Rates

All twenty questions were set as requiring a response and overall completion rates were excellent at 82% or 217 completed responses out of 266 attempts. Overall completion rates would have been higher except that Survey Monkey was set to restrict multiple responses from the same IP address and an issue was reported where the test screenshots did not render on some browsers forcing some respondents to abandon the study.

The survey was initially designed to be completed in under 10 minutes and average completion time was six minutes.

4.3. Demographic Survey

The first half of the study focuses on the profile of respondents with a focus on demographics as deemed relevant from previous studies, online experience, attitudes to privacy and computer self-efficacy as detailed in Section 2.7. The results are detailed in the following section.

4.3.1. Question 1 – Age

The age distribution of respondents is shown in Figure 4-4, below. The sample approaches a normal distribution. By distributing the survey online through traditional and professional social media channels, a skew towards younger participants which is traditionally an issue with third level research was avoided.

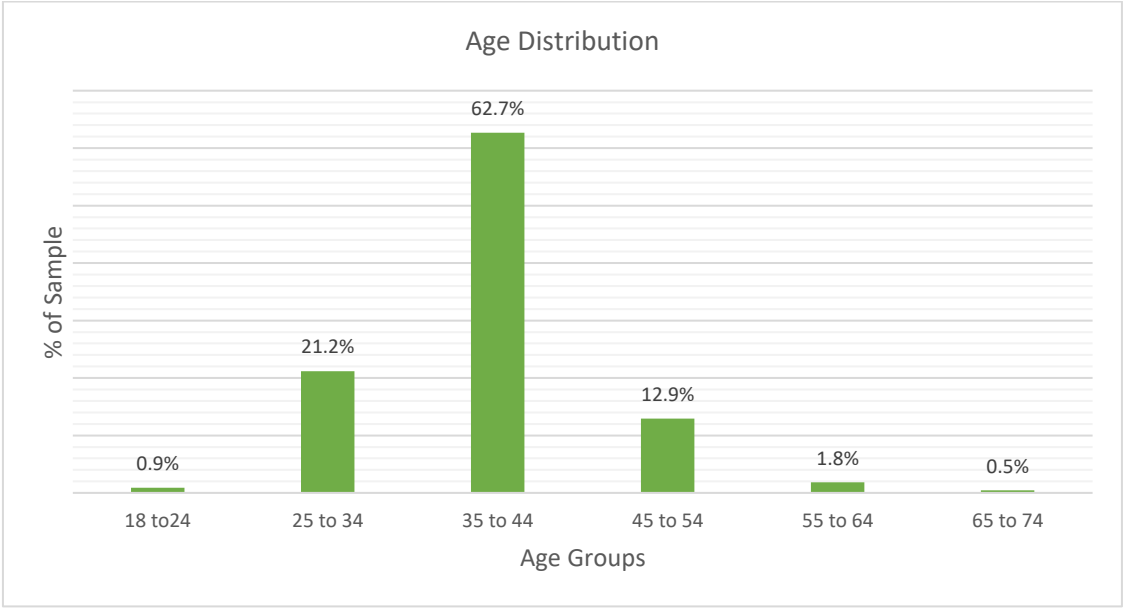


Figure 4-4 - Age Distribution of Survey Respondents

4.3.2. Question 2 – Gender

The pie chart shown below in Figure 4-5 shows the breakdown of male and female respondents. While surveys in the domain of information technology often skew towards a male-dominated sample, female responses in this survey outnumbered male responses by a small margin of 56% to 44%. While this represents a small skew towards females in the sample population, it is a balanced enough sample for this study.

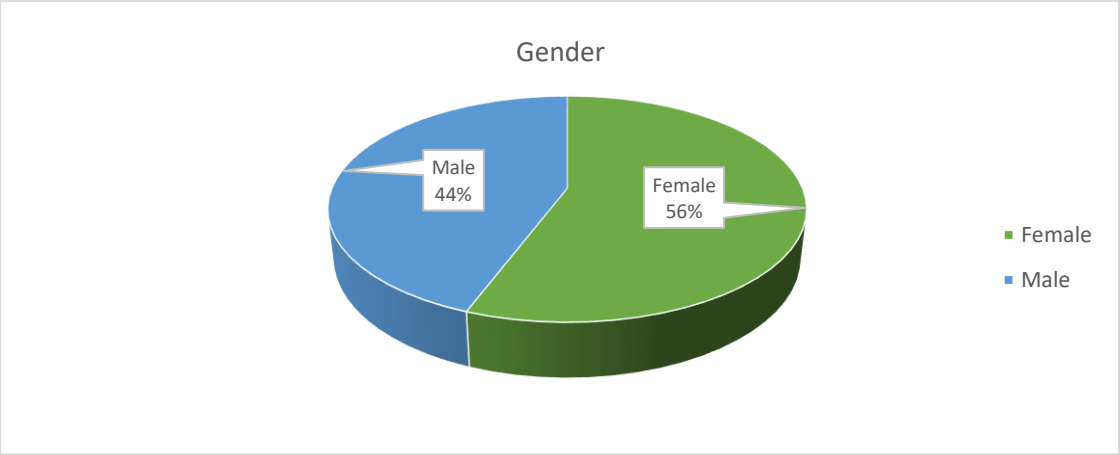


Figure 4-5 - Gender Breakdown of Survey Respondents

4.3.3. Question 3 – Level of Education

Figure 4-6, below, illustrates the highest education level achieved by survey respondents.

The sample approaches normal distribution with a slight skew toward third level education at bachelors and masters degree levels with a combined representation of 70% of the sample.

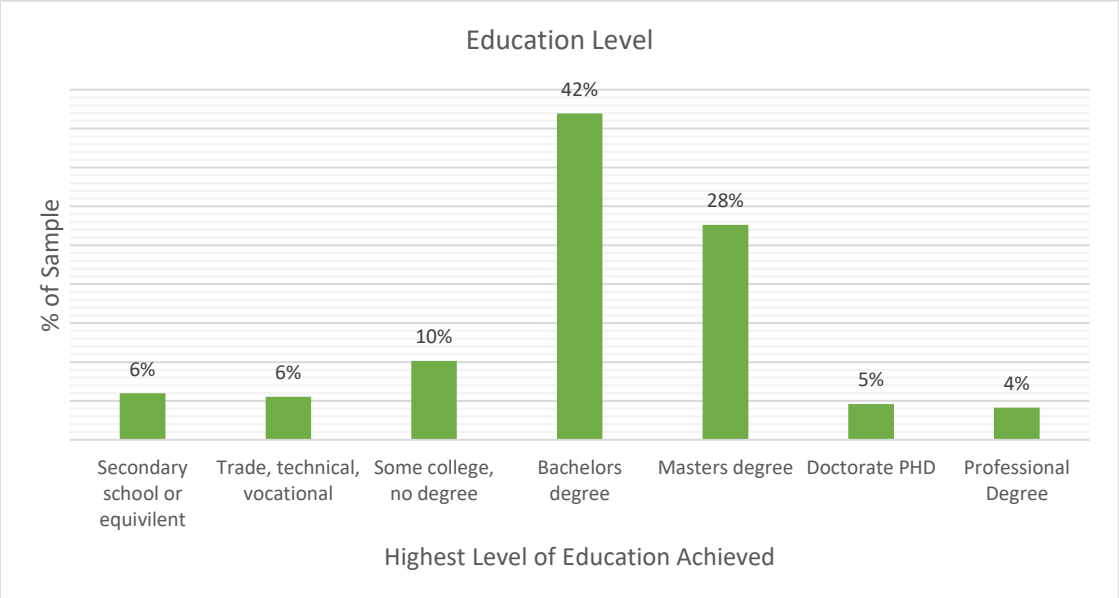


Figure 4-6 - Education Levels of Survey Respondents

4.3.4. Question 4 – Respondent's Field of Work or Study

The areas within which survey respondents work or study are illustrated in Figure 4-7 below. The sample represents a normal distribution.

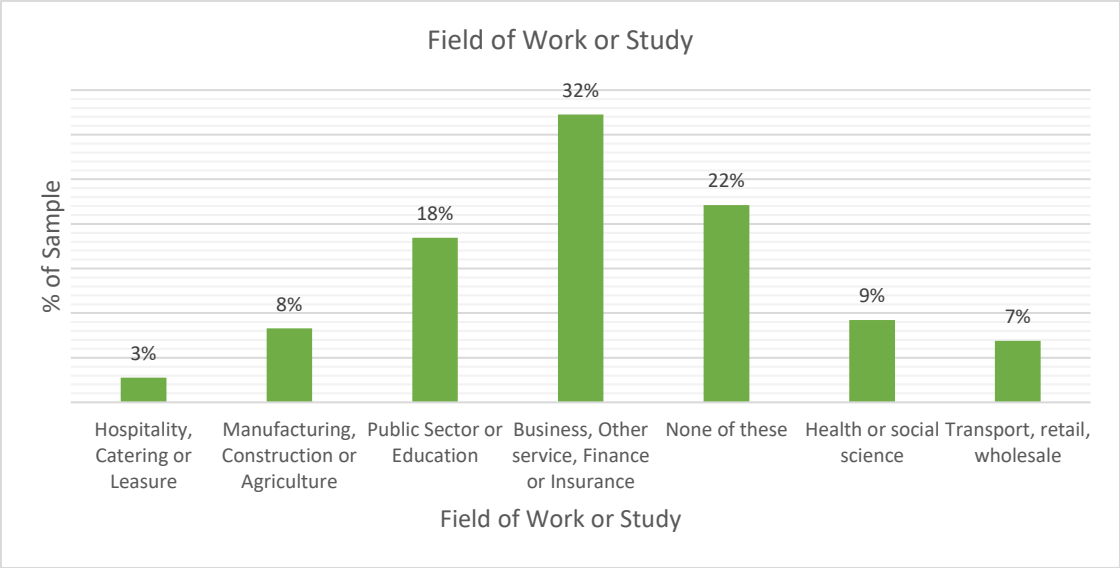


Figure 4-7 - Survey Respondents' Area of Work or Study

4.3.5. Question 5 – Experience of Online Services

Figure 4-8 below, describes survey respondents' experience of online services.

Figure 4-8 - Survey Respondents' Experience of Online Services

The distribution of the sample is not normal, with most respondents indicating experience with virtually all services. This will impact the findings later in the study because the almost uniform usage of all services makes it impossible to assess the impact of prior experience on susceptibility to phishing within the study.

4.3.6. Question 6 – Social Media Usage

Figure 4-9 below shows the social media networks that survey respondents indicated that they use. The sample represents an almost normal distribution with Facebook the most popular platform (94.9%).

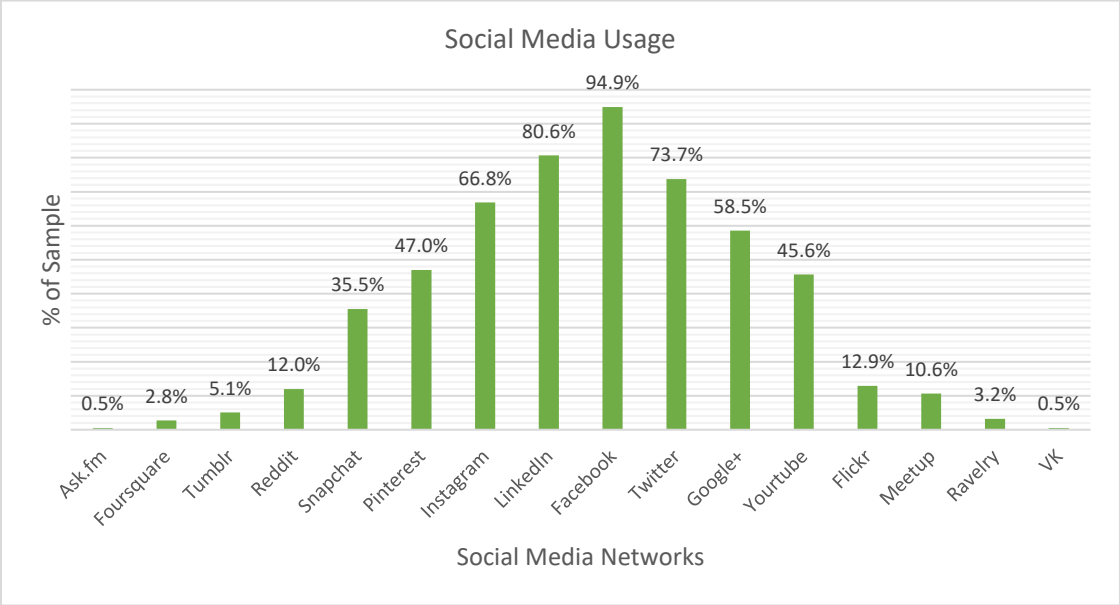


Figure 4-9 - Survey Respondents' Social Media Usage

Respondents were presented with twenty categories, however, four categories with no responses were removed (Odnoklassniki, Qzone, Weibo and None).

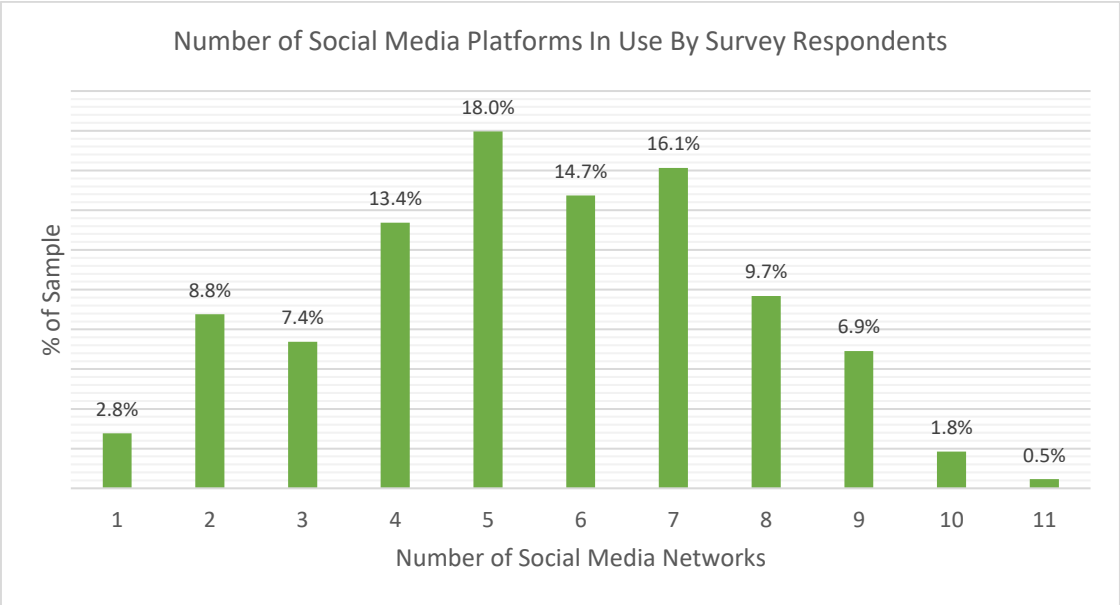


Figure 4-10 - Number of Social Media Platforms Used By Survey Respondents

Respondent data also indicates how many social media platforms respondents were active on (Figure 4-10 on the previous page). This information indicates the respondent's online footprint and the extent to which their personal data is disseminated across the internet. Once again the sample is approaching a normal distribution with the majority of respondents present on between four and seven social media platforms.

As discussed previously, individuals with a high social media presence often display a higher level of trust in online environments and may be more susceptible to phishing. Accordingly, respondents outside this range (3 or less / 8 or more) are assumed to have a lower or higher level of trust, respectively, in online environments and will be examined further in a later chapter.

4.3.7. Question 7 – Social Media Connections In Real Life

Figure 4-11 shows how many of social media connections were known to respondents in real life.

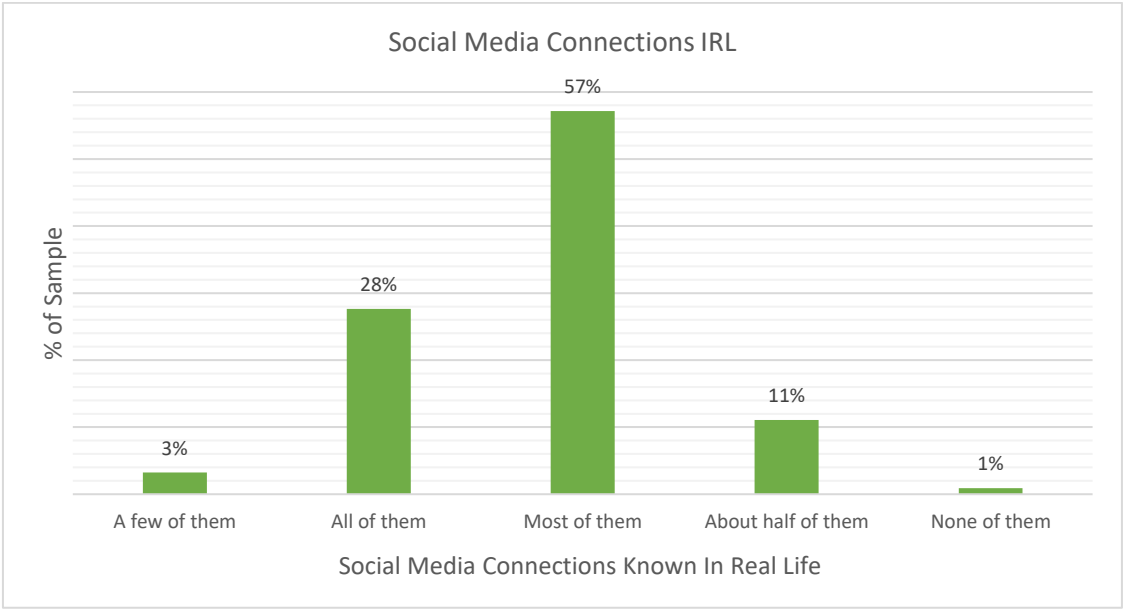


Figure 4-11 - Social Media Connections Known to Survey Respondents In Real Life

This sample again approaches a normal distribution and is used as another indicator of respondent's trust in online environments.

In this case, respondents who stated that they know all or most of their online connections in real life are the benchmarks for a normal level of trust. Those who stated they know about half or less of their online connections in real life are assumed to be more trusting in online environments and will be examined more closely in a later chapter.

4.3.8. Question 8 – Self-Reported Computer Literacy

While not showing a normal distribution in this sample, Figure 4-12, illustrates respondent's self-declared computer literacy, a marker of user experience that can be used to assess their susceptibility to phishing attacks.

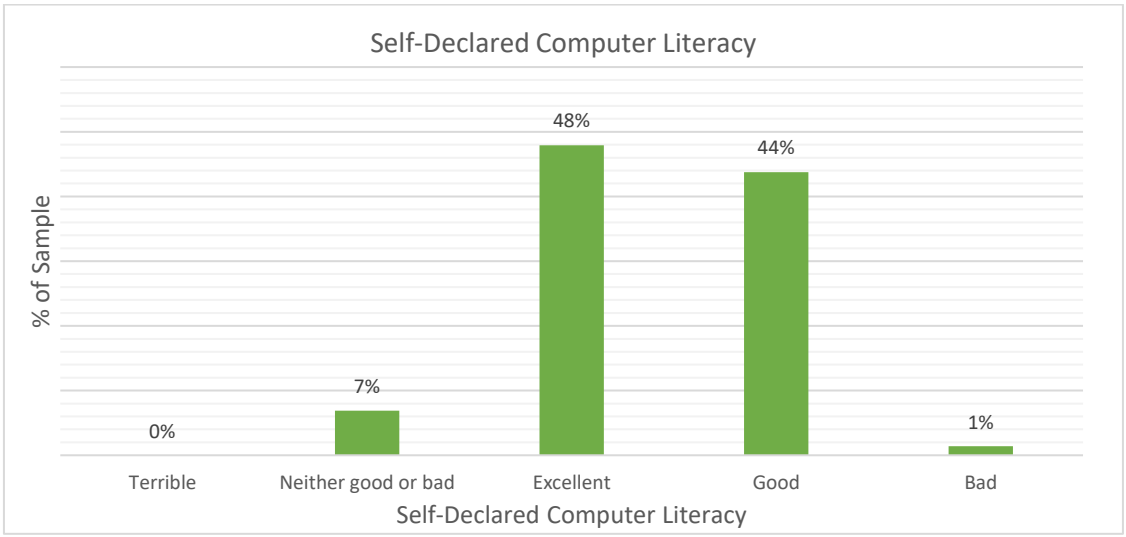


Figure 4-12 - Self-Declared Computer Literacy of Survey Respondents

While most respondent's rated their computer literacy as either "good" or "excellent", a small proportion of respondents declared their computer literacy as "either neither good or bad" or "bad".

Note that no respondents assessed their computer literacy as terrible, a somewhat unsurprising result as the survey and questionnaire were distributed exclusively via social media.

4.3.9. Question 9 – Previous Training

Respondents were asked if they had previously received phishing awareness training and the results are shown in Figure 4-13, below.

Figure 4-13 - Breakdown of Survey Respondents With Prior Phishing Awareness Training

The pie chart shows a broadly even split between those who had received training (43%) and those who had not (55%). There were three respondents (2%) who responded "other", and their answers were as follows:

- "Self-education"
- "Internal email alerts"
- "No official training but have read articles and advisory notices from employer"

It could be argued that these respondents could fall into either of the other categories as there was no definition provided as to what constitutes phishing training within the context of this study. As this question is used as an indicator of both experience and self-efficacy, these respondent's warrant particular attention as they demonstrate an interest in the subject beyond prescribed training.

4.3.10. Question 10 – Expectations of Success

The last question focused on respondents' expectations of success in the phishing test. Figure 4-14, below, shows a sample approaching a normal distribution with most respondents expecting a good performance.

Figure 4-14 - Survey Respondents' Expectations of Success Before Phishing Test

While no respondent's expected to perform terribly, those who expected to perform badly (2%) or neither good nor bad (12%) are of interest due to their lack of self-efficacy in the exercise.

Similarly, those who responded that they expected an excellent performance (24%) display a high degree of self-efficacy and their performance in part 2 is also of particular interest.

5. Results & Analysis

5.1. Phishing Test Results

The second part of the study required respondents to assess a series of ten email screenshots accompanied by a scenario as described in Section 3.3. The ten examples were presented randomly but were designed to assess if respondents focused on technical or content clues when assessing the legitimacy of an email.

5.1.1. Overall Performance

Figure 5-1, below shows how respondents performed during the phishing tests.

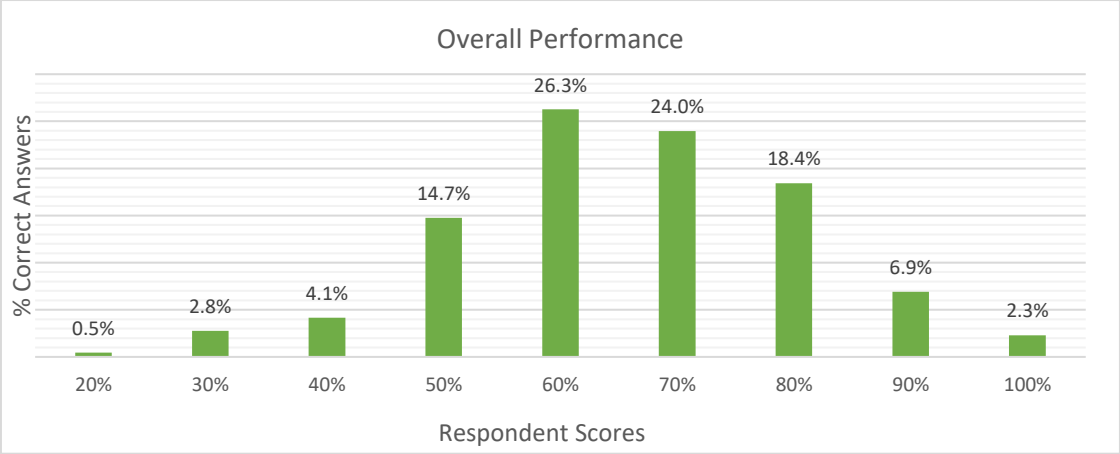


Figure 5-1 - Overall Phishing Test Performance

Score (% Correct Answers)	# of Respondents	% of Respondents	Median	Mean	Std Deviation
0%	0	0.0%	70%	66%	15%
10%	0	0.0%			
20%	1	0.5%			
30%	6	2.8%			
40%	9	4.1%			
50%	32	14.7%			
60%	57	26.3%			
70%	52	24.0%			
80%	40	18.4%			
90%	15	6.9%			
100%	5	2.3%			

Table 5-1 - Breakdown of Overall Phishing Test Performance

No respondents scored below 20% (2/10). Only five respondents (2.4%) received a perfect score of 100% (10/10). The mean score was 66%, and the median score was 70% (7/10). As such, above average performance is a score of 80% or over (27.6% of the sample) and below average performance is a score of 50% or below (22.1% of the sample) as shown in Table 5-1.

Figure 5-2 below, shows the overall breakdown of answers to each question. Those who answered correctly are represented in green, those who answered incorrectly in blue, and those that didn't know represented in yellow.

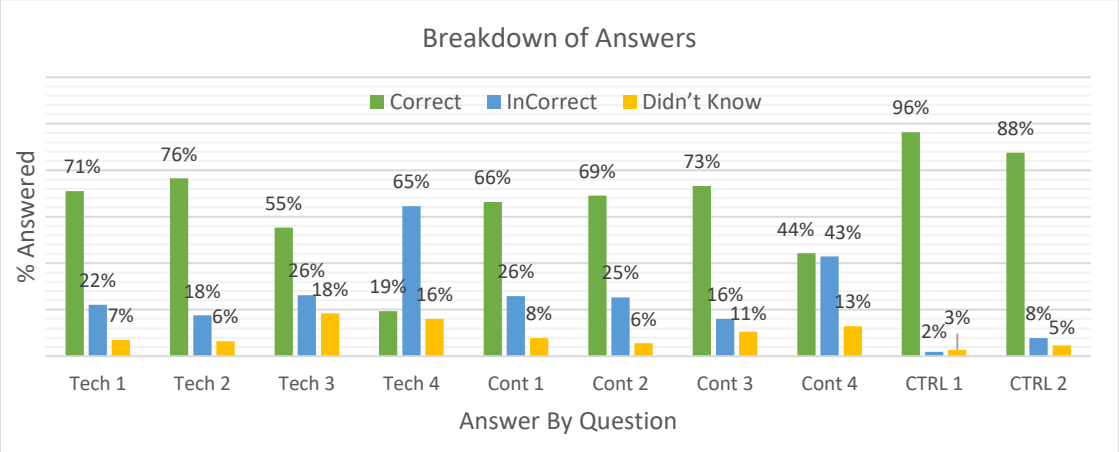


Figure 5-2 - Breakdown of Respondents Answers By Question

Performance across the technical and content-focused questions was broadly the same. Interestingly, both genuine examples (Tech 4 & Cont 4) showed significantly worse results as illustrated in Figure 5-3.

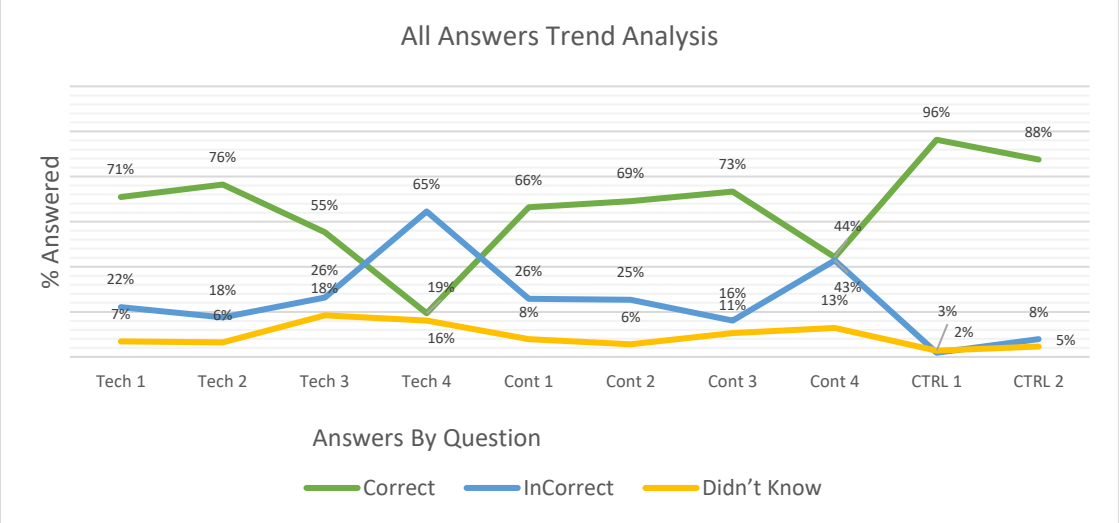


Figure 5-3 - Trend Analysis of All Answers by Question.

While both examples are genuine, each contains a somewhat suspicious technical or content element. The Parcel Motel example (Tech 4) contains a domain not easily associated with Parcel Motel, and the Netflix example (Cont 4) contains a salutation and other details that could be viewed as not in keeping with a customer-focused communication to the sender.

This shows that respondents will err on the side of caution if presented with any elements that seem to undermine the legitimacy of the email even is all the other indicators of legitimacy are

present. This finding is echoed by respondents' performance across the two control questions (CTRL 1 & CTRL 2) as shown in Figure 5-4 below.

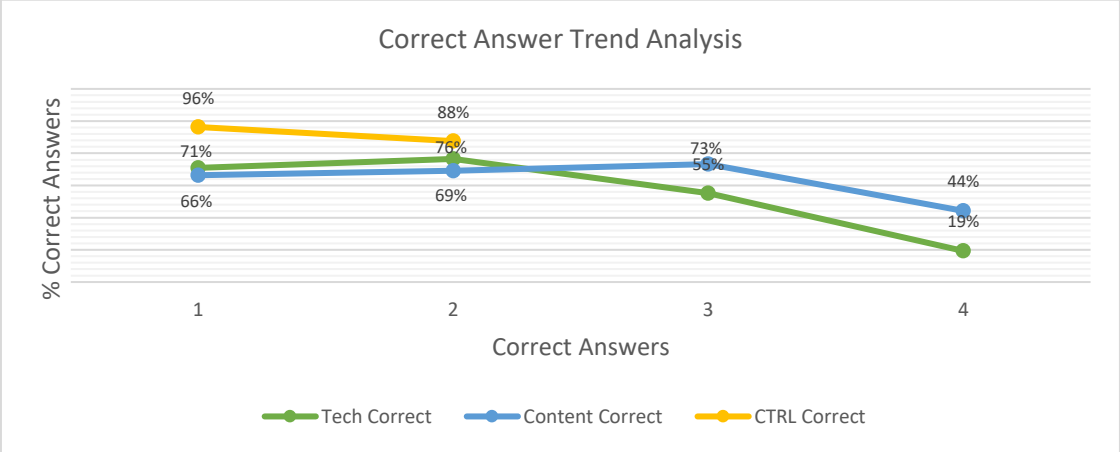


Figure 5-4 - Trend Analysis of Correct Answers By Category

The Facebook example (CTRL 1) was designed to be obviously fraudulent while the 123.ie example (CTRL 2) was designed to be clearly genuine with scenarios provided for reinforcement in each case. While respondents performed better on these questions with 98% and 88% success respectively, the genuine example still shows a lower score than the phishing example, again indicating that respondents are prone to false positives in these scenarios.

5.1.2. Demographics

The demographic portion of testing assesses how respondents from different demographic sets performed across the phishing test examples.

5.1.2.1. Age

Figure 5-5 shows correct answers to all questions by age group and their deviation from the average score of 66%.

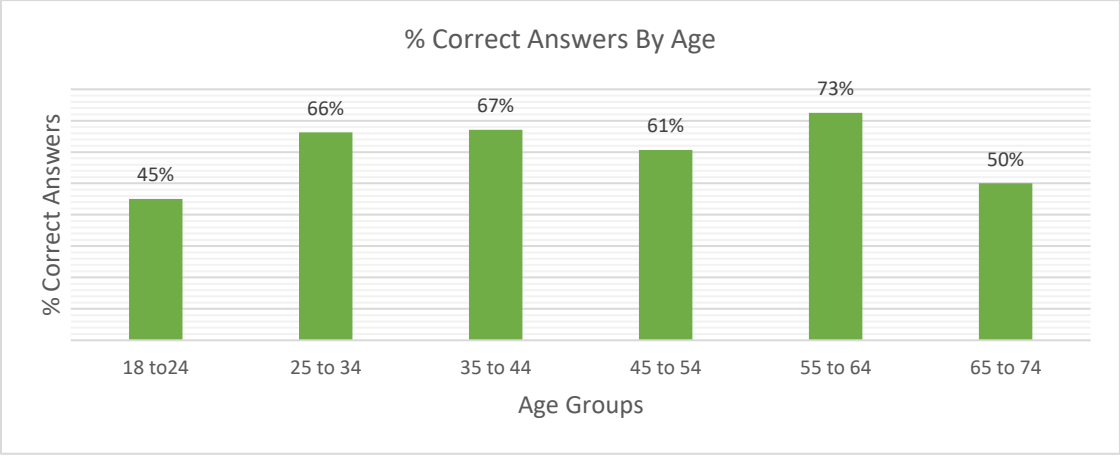


Figure 5-5 - % Correct Answers By Age

While the “18 to 24” and “65 to 74” categories performed worse across all questions, and the “55 to 64” category performed best, their sample sizes are too small to derive statistically significant meaning from the results. Removing these and focusing on the age ranges with a sufficiently large sample (“25 to 34”, “35 to 44” & “45 to 54”) shows that the “45 to 54” category performed statistically worse across all tests indicating that age may be a factor with regards to susceptibility to phishing.

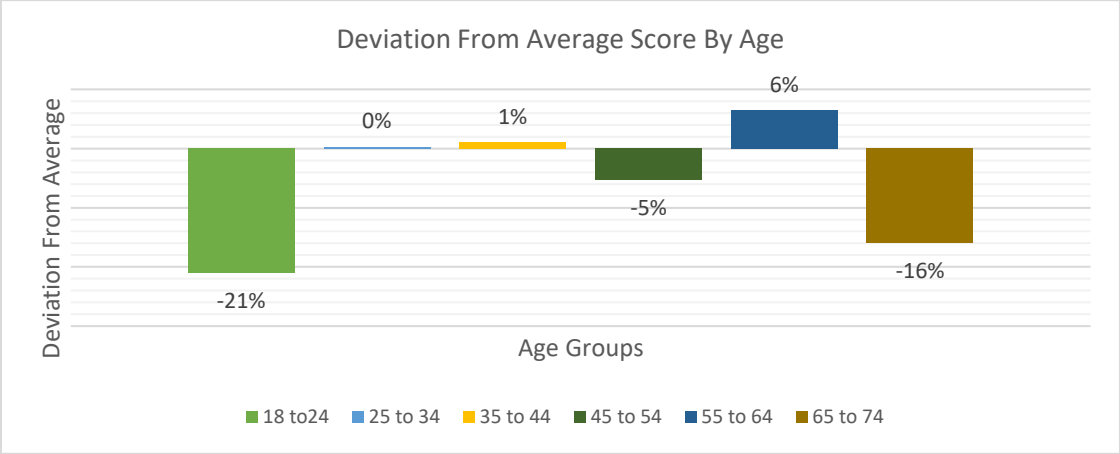


Figure 5-6 - Deviation From Average Score By Age

5.1.2.2. Gender

Correct answers by gender and their deviation from the average score are shown in Figure 5-7.

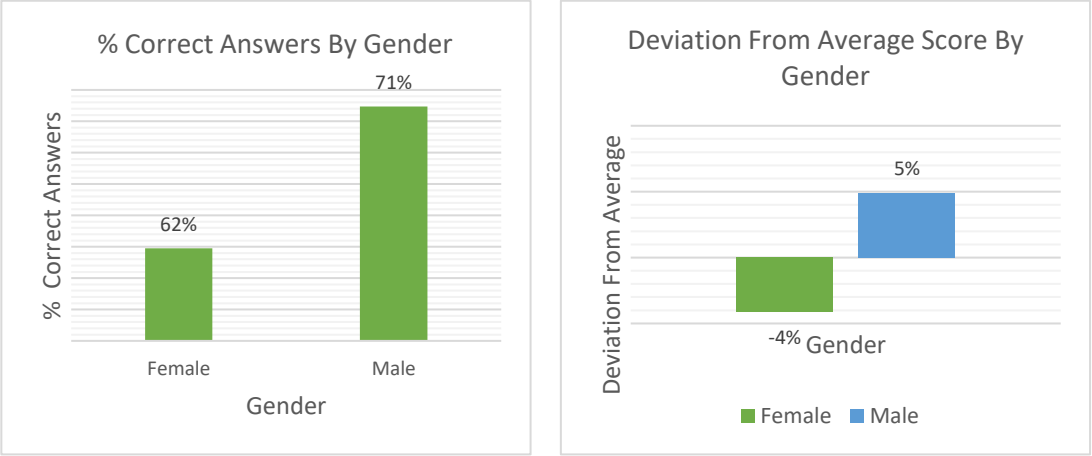


Figure 5-7 - % Correct Answers And Deviation From Average By Gender

With a sample ratio of 56:44, female: male, the performance of male respondents with an average score of 71% versus female respondents with an average score of 62% is statistically significant.

Males in the study performed 9% better overall than females and 5% above average as a whole. This finding supports previous studies that have shown female respondents to be more susceptible to phishing attacks than males.

5.1.2.3. Education

Figure 5-8 and Figure 5-9, below and on the next page, show correct answers by level of education and their deviation from the average correct score of 66%.

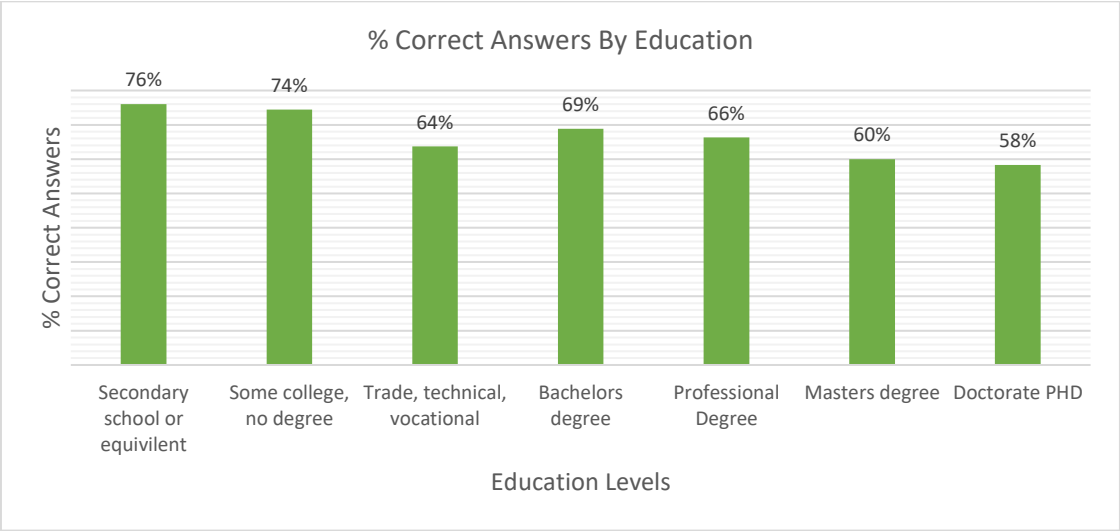


Figure 5-8 - % Correct Answers By Education

While the majority of respondents held bachelors or masters degrees, other education levels were well represented within the sample. Significantly, respondents with lower education levels ("secondary school" or "some college but no degree") performed significantly better than those with the highest levels of education ("masters" and "doctorate PhD").

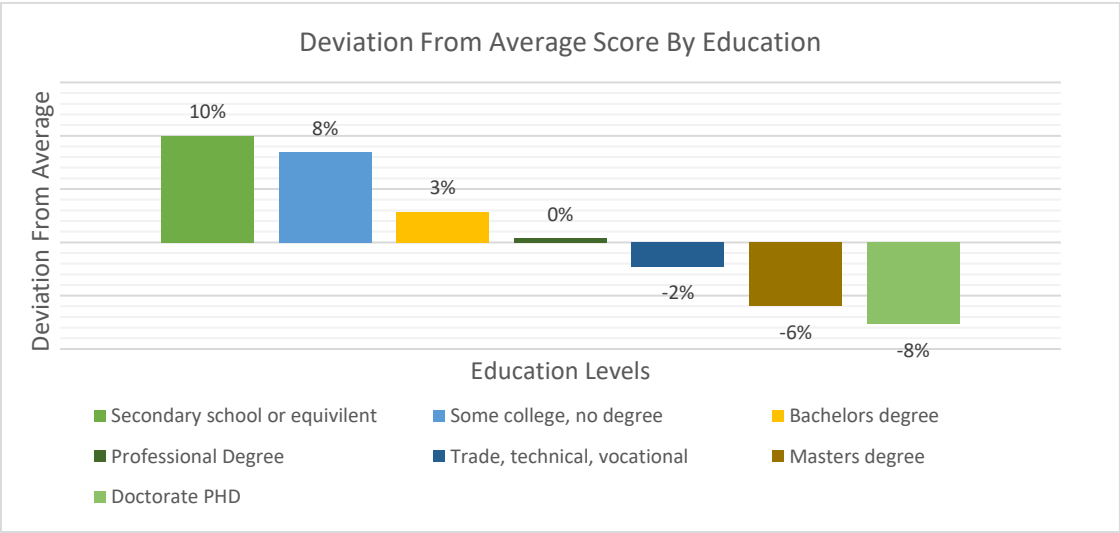


Figure 5-9 - Deviation From Average Score By Education

The gap is significant with secondary school or some college but no degree categories performing at 10% and 8% above average respectively versus 6% to 8% below average for masters and doctorate holders respectively.

5.1.2.4. Area of Work or Study

Figure 5-10 and Figure 5-11 show correct answers and deviation by field of work or study.

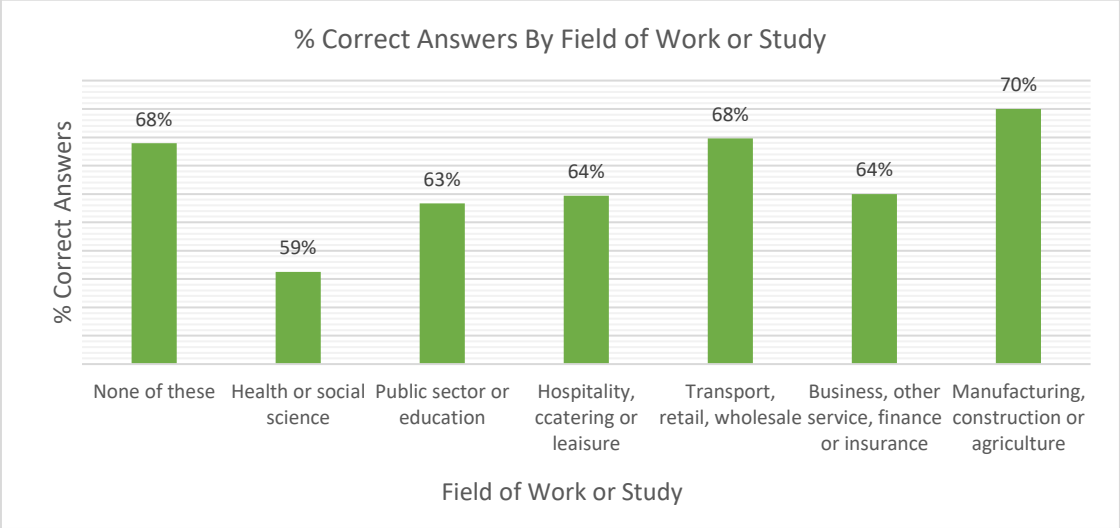


Figure 5-10 - % Correct Answers By Field of Work or Study

As the chart shows, respondents working in manufacturing, construction or agriculture performed 4% above average while respondents from the health or social science area performed 8% below average.

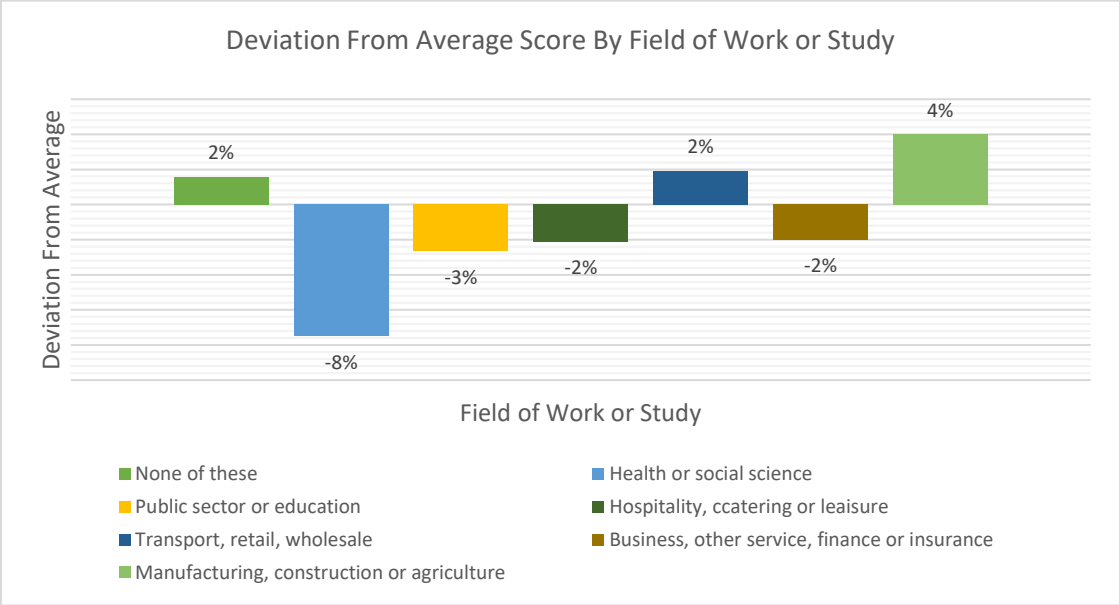


Figure 5-11 - Deviation From Average Score By Field of Work or Study

This is an interesting finding as respondents from either sector would be less exposed to email on a daily basis than those from other sectors such as business, finance or insurance.

5.1.3. Online Experience

This section examines if respondents with prior experience of the services used as part of the testing performed better than those without prior experience.

5.1.3.1. Experience of Online Services

Figure 5-12 below shows the average number of online services associated with respondents correct answers. This question was intended to examine if previous experience of a service correlated with a higher success rate in detecting a phishing emails associated with that service. Unfortunately this was impossible to answer based on the profile of the sample.

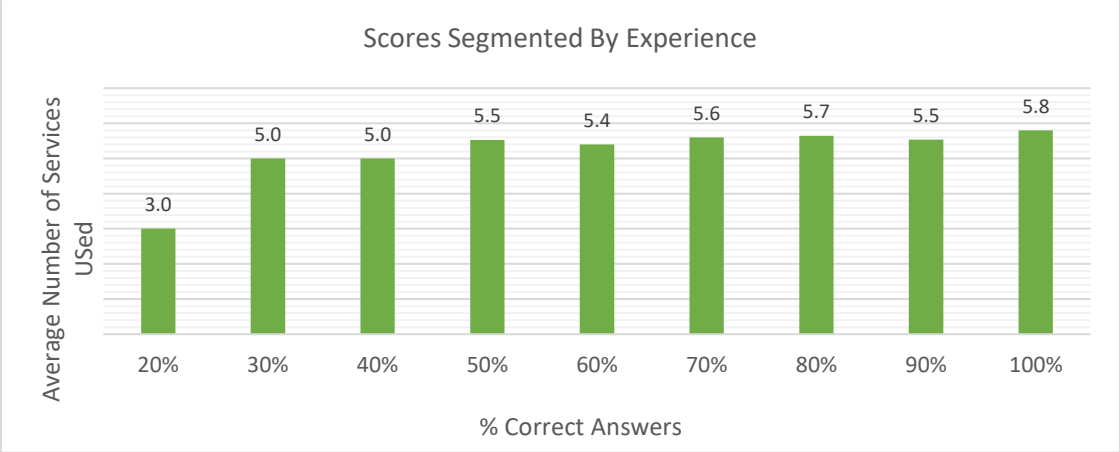


Figure 5-12 - Scores Segmented By Experience

A higher level examination of the data does, however reveal a trend between the lowest and highest performing respondent groups as shown in Figure 5-13wi on the following page, with the lowest performers (20% – 40% correct) using an average of 4.33 out of the 6 services listed versus 5.66 out of 6 services listed for the highest performers (80% - 100% correct). This indicates that online experience may play a part in helping users identify phishing emails.

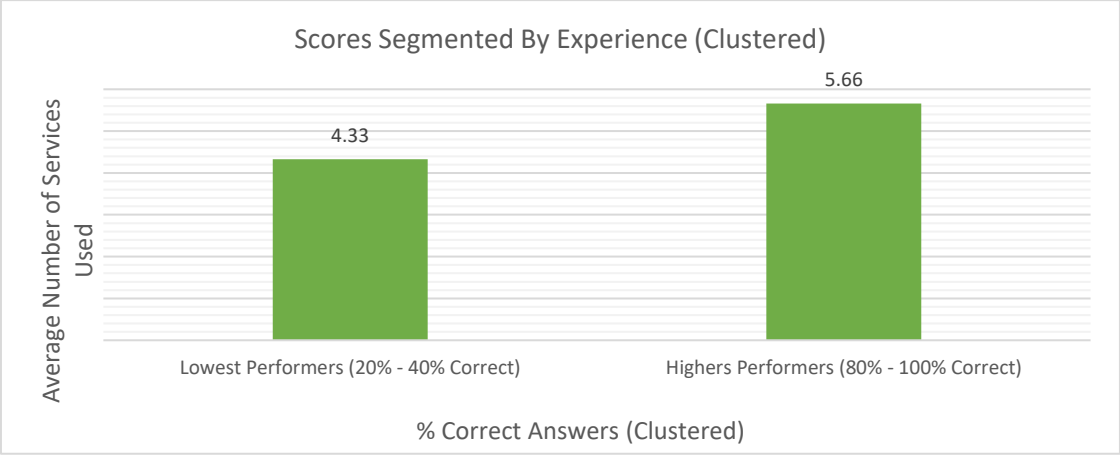


Figure 5-13 - Scores Segmented By Experience (Clustered)

5.1.4. Attitude To Privacy

Attitude to privacy is derived from two metrics, the number of social media platforms upon which respondents are present, and how many connections respondents stated they had in the real world. Respondents with a presence on a large number of social media platforms as well as those with fewer connections known to them in real life are deemed to have a lesser expectation of privacy and a higher trust in the online world.

5.1.4.1. Social Media Usage

Figure 5-14, below, shows the average number of social media networks per respondent based on their correct answers in the phishing test.

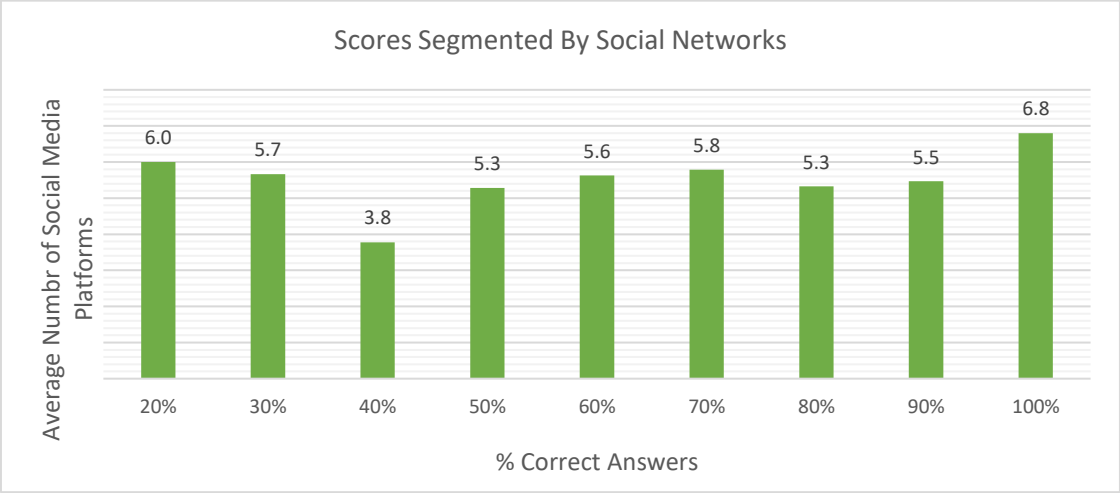


Figure 5-14 - Scores Segmented By Social Media Networks

As evidenced by Figure 5-15, there is no clear trend in this instance. Both the worst and best performers are present on more platforms than the average performers (9% and 23% respectively).

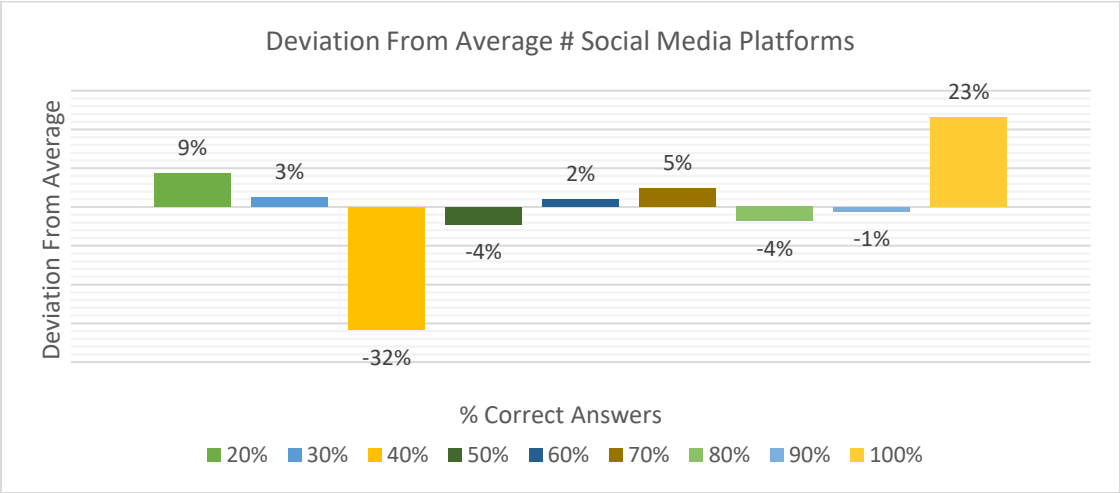


Figure 5-15 - Deviation From Average, Social Media Platforms By Correct Answer

The inconclusive nature of results is also apparent when examining the average score based on the number of social media accounts in use as shown in Figure 5-16 below.

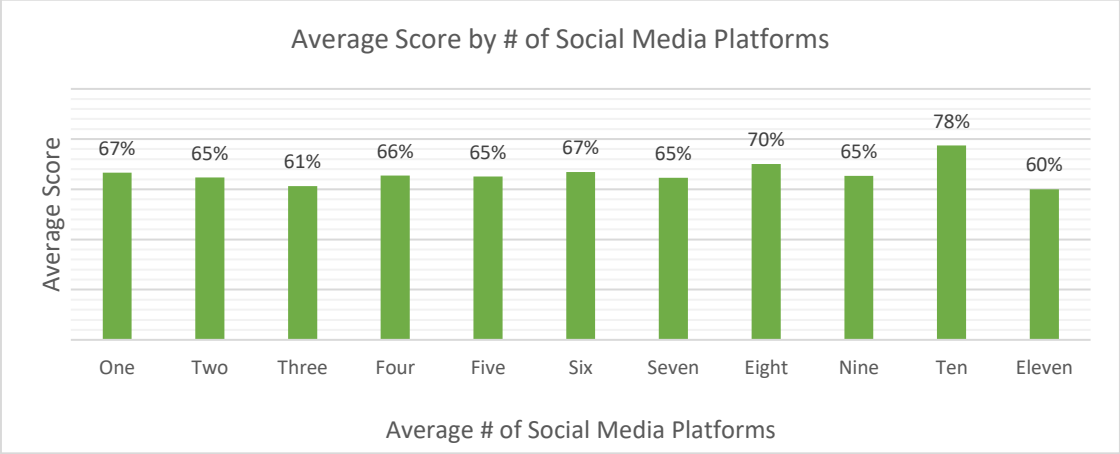


Figure 5-16 - Average Score by Social Media Platform Use

This chart shows that those with the most social media connections (10 and 11) scored, on average the best (78%) and worst (60%) respectively. Furthermore, the range is so small across the board that it is impossible to show any statistically significant trend within the data.

5.1.4.2. Connections In Real Life

Figure 5-17, below, shows average performance by respondents grouped by the number of connections from social media networks they estimated to have a relationship with in real life.

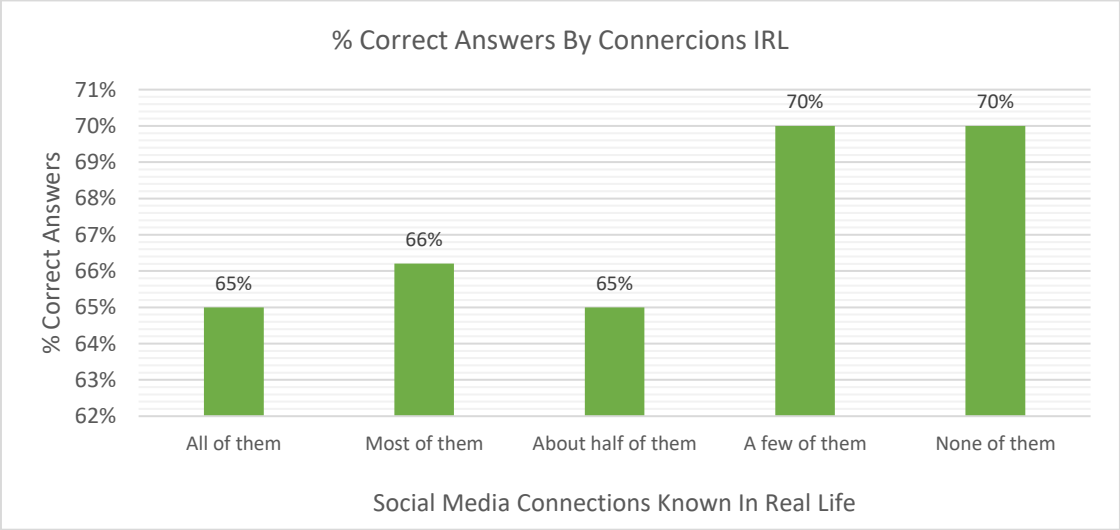


Figure 5-17 - % Correct Answers By Social Media Connections IRL

The graph above illustrates that those that declared that they only knew a few or none of their online connections in the offline world performed significantly worse than the rest of the sample across the phishing tests, however this represents a relatively small portion of the sample (11%) and may not be statistically significant as a result.

5.1.5. Self-Efficacy

This section examines success rates based on respondents' self-declared computer literacy, previous training and expectations of success.

5.1.5.1. Computer Literacy

Figure 5-18 below, shows average performance by respondents based on their self-declared computer literacy.

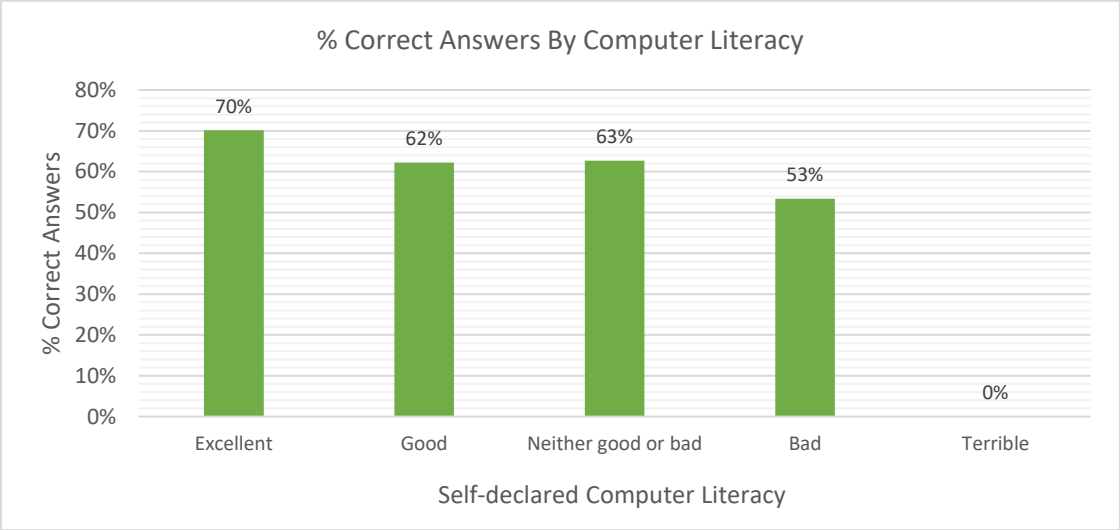


Figure 5-18 - % Correct Answers By Computer Literacy

The graph illustrates that those who self-identified as having good computer literacy (rating "excellent" or "good") outperformed those with less knowledge in the area. Significantly, as shown in Figure 5-19 below, those who claimed to have excellent computer literacy performed 4% above average which indicates that overconfidence was not a factor with these respondents.

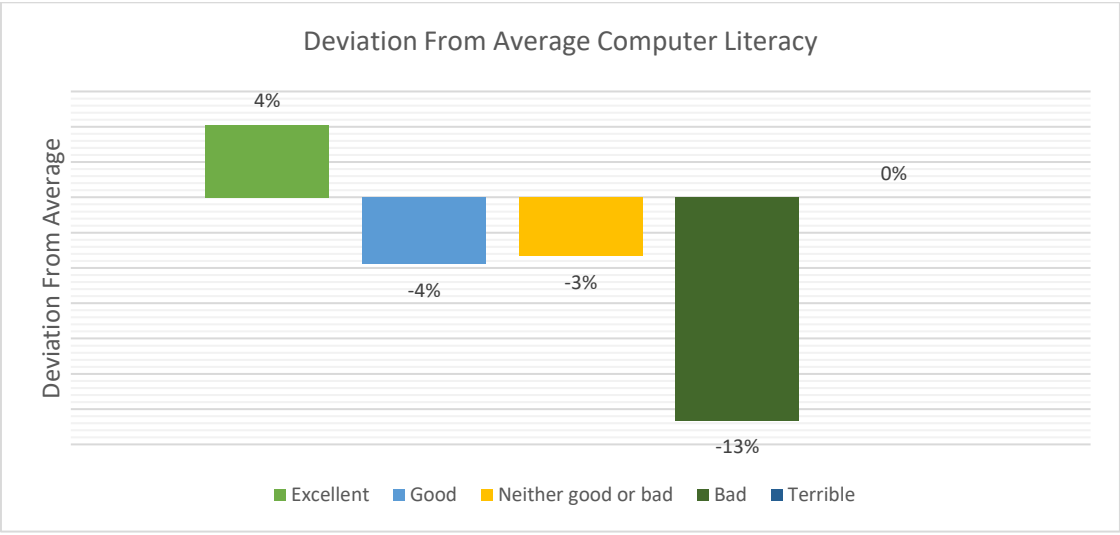


Figure 5-19 - Deviation From Average Score by Computer Literacy

Interestingly, all other respondents performed below average with those who declared their computer literacy to be “bad” at 13% below average, those who selected “neither good or bad” at 3% below average, and those that selected “good” at 4% below average. While 48% of the sample declared their computer literacy to be “excellent”, 44% selected “good”, making this finding statistically significant.

5.1.5.2. Previous Training

Figure 5-20, below, shows average performance based on previous training. In the original sample, 43% of respondents had previously received phishing awareness training versus 55% who had not (2% or respondents selected “other”)

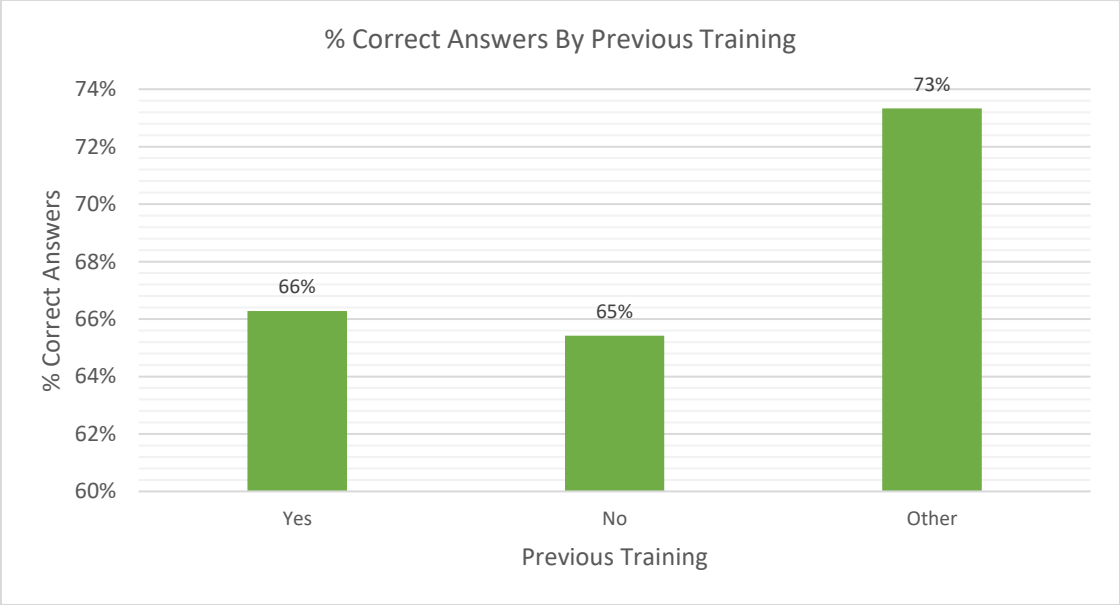


Figure 5-20 - % Correct Answers By Previous Training

As the chart above illustrates, those who had previously received training, and those who had not, performed at almost exactly the same level with previously trained respondents performing at exactly the average level of 66% and those not previously trained performing just 1% worse at 65%.

Respondents who selected “other”, citing sources such as self-teaching or reading email alerts and journals performed significantly better however with a sample size of 3 respondents, just 2% of the sample, it is impossible to derive statistical significance from these figures.

The findings from this section indicate that phishing awareness training may be ineffective with no appreciable difference in performance between either group.

5.1.5.3. Expectation of Success

Figure 5-21 below, shows performance by respondents based on their expectations of success in the phishing test. This question was asked prior to participants seeing any of the test examples and shows that the more confident respondents performed the best.

Figure 5-21 - % Correct By Expectation of Success

This is evident in Figure 5-22 below, which shows that those who expected an excellent or good result performed 7% and 4% respectively above average while all other subject performed below average. This is statistically significant because 24% of the sample predicted an excellent result versus 62% who chose "good". The remaining respondents make up 14% of the overall sample.

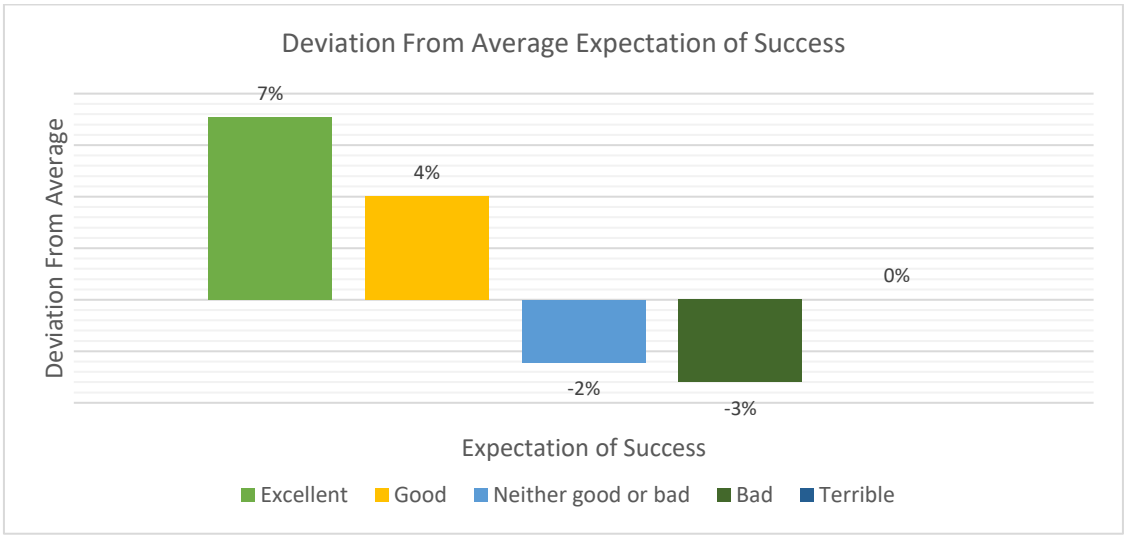


Figure 5-22 - Deviation From Average Score By Expectation of Success

5.2. Summary of Phishing Test Results

This section recaps the initial findings from the survey and test as summarised in Table 5-2 below. Findings are summarised by category.

Question #	Group	Description of Findings	Best Performers	Worst Performers	Category	
Overall	Overall Results	Average score of correct answers was 66% across all respondents with a median score of 70%	Respondents with a score of - 20% - 50%	Repspondents with a score of 80% - 100%	***Overall***	
1	Age	Evidence that age may be a factor in susceptibility to phishing attack	Respondents in age categories "25 - 34" and "35 - 44"	Respondents in age categories "45 - 54"	***A. Demographic Grouping***	
2	Gender	Evidence that gender may be a factor in susceptibility to phishing	Male respondents	Female respondents		
3	Education	Evidence that education levels may be a factor in susceptibility to phishing attack	Respondents in education categories "secondary school or equivilent" and "some college, no degree"	Respondents in education categories "masters degree" and "doctorate phd"		
4	Field of Work or Study	Evidence that field of work or study may be a factor in susceptibility to phishing attack	Respondents in industry categories "none", "transport, retail, wholesale" and "manufacturing, construction or agriculture"	Respondents in industry categories "health & social science", "public sector & education", "hospitality, catering & leisure" and "business, other services, finance or insurance"		
5	Experience of Online Services	Unable to assess if experience of individual services has a positive or negative impact on susceptibility to phishing Some evidence that overall experience has some impact on phishing susceptibility	Respondents with experience of 6 or more of the services	Respondents with experience of 4 or less of the services	***B. Experience***	
6	Social Medial Usage	No significant findings	N/A	N/A		***C. Attitude to Privacy***
7	Connections IRL	No significant findings	N/A	N/A		
8	Computer Literacy	Evidence that computer literacy may be a factor in susceptibility to phishing attack	Respondents who declared their computer literacy as "excellent"	All other respondents		***D. Computer Self-Efficacy***
9	Previous Training	No significant findings	N/A	N/A		
10	Expectations of Success	Evidence that self-efficacy may be a factor in susceptibility to phishing attack	Respondents who declared their expectation of success as "excellent" or "good"	All other respondents		

Table 5-2 - Summary of Initial Findings

5.2.1. Overall Results

The average test score across the test was 66% with a median score of 70% (7 correct answers out of 10). A total of five respondents scored 100%, all of whom were male. Above average performance is a score of 80% or over (27.6% of the sample) and below average performance is a score of 50% or below (22.1% of the sample).

Respondents showed no performance difference across the technical or content focused tests however respondents performed poorest when assessing the genuine examples. This indicates that participants may not possess the skills to accurately assess the legitimacy of an email as indicated in earlier studies described in the literary review.

5.2.2. Demographics

The study indicates that age may be a factor in determining individuals susceptibility to phishing, finding that respondents in the "25 to 34", "35 to 44" & "45 to 54" categories performed better than older participants in the "45 to 54" category. This supports the hypothesis that older internet users are most at risk from phishing scams.

The findings from the study also support the theory that men are less susceptible to attack than women with men scoring an average of 71% versus 62% for women.

Respondents with lower levels of education performed better than those with higher level qualifications, the best performers being those with an education level of "high school or equivalent" or "some college but no degree". Respondent's with Masters degrees or PhDs faired statistically worse supporting the hypothesis that highly educated individuals may be more susceptible to phishing attacks than those with lower levels of education. While one theory cites over-confidence as a factor with highly educated individuals, this finding is not supported by the performance of respondents who showed confidence in their ability before the test or declared a high level of computer literacy.

Finally, there was evidence that the field of work or study within which the respondents categorised themselves may be a factor in their susceptibility to phishing. Interestingly, participants from industries that would traditionally involve more manual labour outperformed those who would be more likely to use email and computers as part of their daily routine.

5.2.3. Experience

Initially, it was hoped to assess if prior usage of a particular type of online service, such as online shopping, banking or media streaming, would impact on respondents' ability to correctly assess test examples in that category, for example, Amazon, AIB Bank or Netflix respectively. Unfortunately, most respondents indicated prior use of practically all services making this impossible to assess.

There was evidence, however, that respondents with the lowest level of usage across these services also performed worse than those with higher usage statistics. In addition, other secondary indicators of online experience, such as information regarding social network usage and the number of social media connections known to participants in real life proved inconclusive (see section 5.2.4 below).

The study found no difference in performance between participants who had received phishing awareness training and those who had not, indicating that current methods of training may be ineffective.

There is some evidence that self-declared computer literacy may be an indicator of susceptibility to phishing (see section 5.2.5 below), however this study fails to reveal any additional insight into the role of experience in susceptibility to phishing.

5.2.4. Attitude to Privacy

It was hoped that the amount of social media networks respondents were present on, as well as the number of connections they knew in real life, could be used to gauge participant's levels of trust and expectations of privacy in online environments. As discussed in the literary review, previous research suggests that these metrics can be used infer individuals attitude to privacy. Comparing respondents performace based on this information could indicate if attitude to privacy might be a factor in susceptibility to phishing. Unfortunately, this study returned no statistically significant results and therefore failed to reveal any additional information in this area.

5.2.5. Computer Self-Efficacy

Self-efficacy is confidence in one's ability to complete a task or derive a positive outcome to an event. Its effect on phishing susceptibility is discussed in the literature and suggests that individuals who believe they can successfully identify a fraudulent email often do so.

In this study, respondents' self-declared computer literacy and whether or not they had previously received phishing awareness training were used as indicators of the participant's self-efficacy. The last question in the survey then simply asked participants how they expected to perform in the test, with this answer an absolute measure.

The study shows that participants who rated their computer literacy as "excellent", out-performed all other participants. Similarly, those that stated that they expected their performance in the test to be excellent, also out-performed all other participants. Evidence from the study suggests, therefore, that computer self-efficacy may indeed be a factor in determining individuals susceptibility to phishing attacks.

Interestingly, there was no statistically significant difference between the performance of respondents who had previously received training and those who had not, suggesting that such training is largely ineffective.

5.3. Further Investigation Into Information Processing

The previous section described the basic findings from the study, examining how demographics and other less quantifiable factors such as experience, attitude to privacy and computer self-efficacy may play a part in an individuals susceptibility to phishing attacks. This lead to the identification of some statistically significant results across the sample. The second question posed at the beginning of this study was if different groups process information differently when assessing the legitimacy of an email. This section attempts to answer this question.

5.3.1. Methodology

The best and worst performing groups are described in Table 5-2 - Summary of Initial Findings, in the previous section. To investigate how each group processes data, it is necessary to compare their results on the technical phishing test against their result on the content-based ones. Note that the two control emails are excluded from this part of the assessment.

By comparing each groups performance in this way, the study will establish if there is a pattern of behaviours within the individual groups and a trend of behaviour across the groups collectively. If the study finds that one group is more or less successful in correctly determining the legitimacy of a specific type of email (technical or content-focused), the inference will be that this group is more reliant on this type of an indicator than the other. This part of the study was conducted as follows.

- First, the best and worst performers are selected from each group where a statistically significant result was found.
- Then, the worst performers average performance across the four technical examples was averaged and compared with their average performance across the four content examples.
- These results were then normalised to generate a ratio, represented by a pie chart for illustration purposes.
- Once completed for each category, the overall results were correlated in the same manner to provide a comparison of the groups of worst and best performers overall.

If the success rates across the technical and content-focused phishing examples are found to be 50:50, it will indicate no difference in how each group processed information. Alternatively, a ratio indicating a bias towards either technical or content related indicators will suggest that users from that category focus on one or the other when evaluationg the legitimacy of an email.

The results of this comparison are described in the following section.

5.3.2. Performance Comparisons Between Best and Worst Performers

This section compares the performance of the best and worst performing groups against the technical and content related phishing tests. The individual results for each statistically significant group, as identified in previous chapters, as well as an overall comparison based on the groups combined, are summarised in Table 5-3 and Table 5-4 below. These results are discussed in the following paragraphs.

Worst Performers	Technical	Content
Lowest Scores Overall (30% - 40%)	58%	42%
Lowest Scores by Age (45 to 54)	49%	51%
Lowest Scores by Gender (Female)	43%	57%
Lowest Scores by Education (MS / PHD)	47%	53%
Lowest Scores by Field of Work or Study (Health or Social Science)	43%	58%
Lowest Scores by Computer Literacy ("Good")	47%	53%
Lowest Scores by Expectation of Performance "Good")	47%	53%
AVERAGE	48%	52%

Table 5-3 - Comparison Table of Worst Performers

Best Performers	Technical	Content
Highest Scores Overall (90% - 100%)	45%	55%
Highest Scores by Age (35 to 44)	46%	54%
Lowest Scores by Gender (Male)	50%	50%
Highest Scores by Education (School / Some College)	47%	53%
Highest Scores by Field of Work or Study (Manufacturing, Construction or Agriculture)	51%	49%
Highest Scores by Computer Literacy ("Excellent")	47%	53%
Highest Scores by Expectation of Performance ("Excellent")	47%	53%
AVERAGE	48%	52%

Table 5-4 - Comparison Table of Best Performers

5.3.2.1. Comparison Results By Overall Score

The comparison between respondents with the lowest overall scores (20% - 40%) and those with the highest (90% - 100%) is shown in Figure 5-23 below.

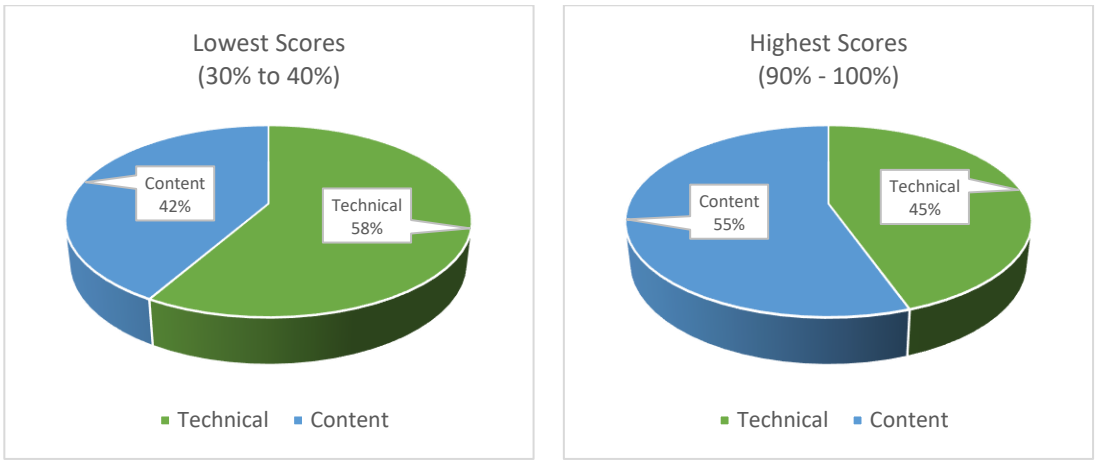


Figure 5-23 - Comparison Results By Overall Score

The pie charts above show that respondents with the lowest overall scores show a definite bias towards the technical clues (42:58, content:technical) indicating that the technical elements of

the test examples were the main focus for this group of respondents. In contrast, the most successful respondents overall, appear to have evaluated all elements of the email examples, with only a very slight bias towards the content of the email over the technical clues with a split of 55:45 (content: technical) in favour of content.

5.3.2.2. Comparison Results By Age

The comparison between highest and lowest scoring respondents by age is shown in Figure 5-24 below.

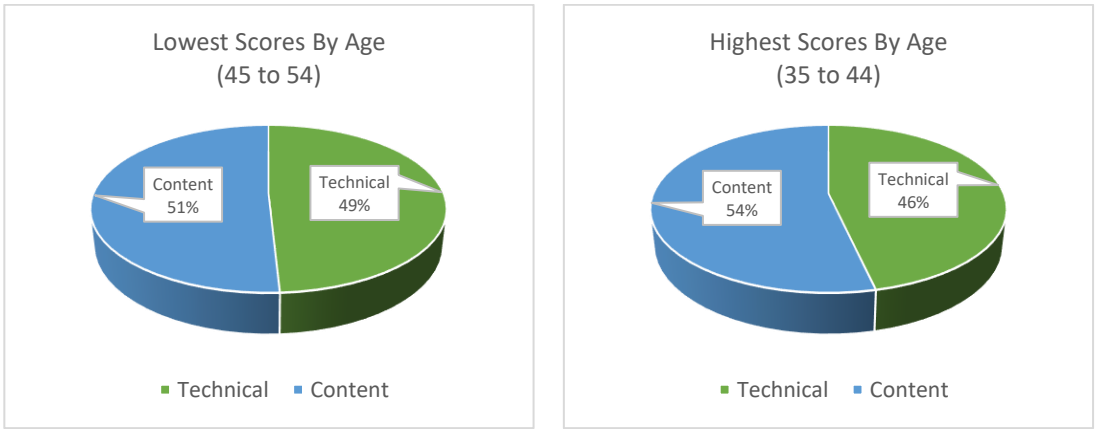


Figure 5-24 - Comparison Results By Age

The pie charts above show that the worst performers in this category performed equally well across technical and content-focused examples with a ration of 51:49 (content:technical).

The best performers exhibited a slight bias towards content with a ration of 54:46 (content:technical) indicating that the most successful respondents in this category also favoured content clues by a small margin.

5.3.2.3. Comparison Results By Gender

The comparison between highest and lowest scoring respondents by gender is shown in Figure 5-25 below.

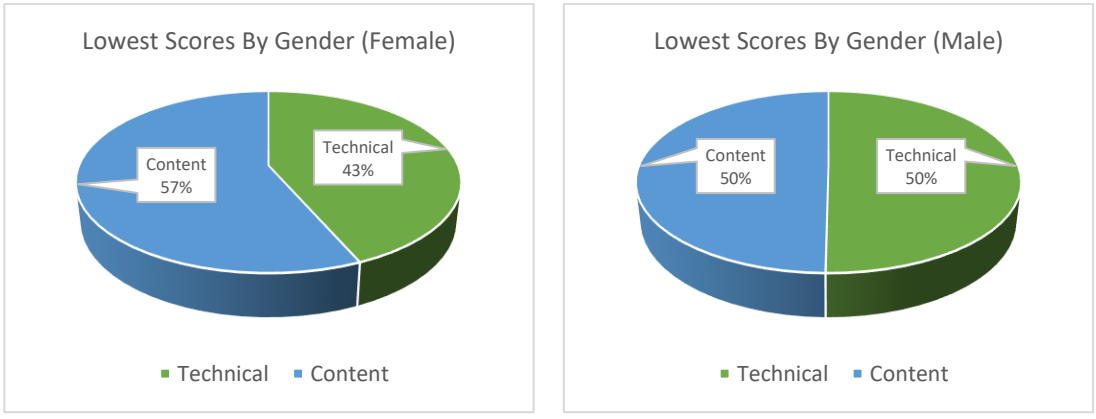


Figure 5-25 - Comparison Results By Gender

The worst performers in this instance were female participants. The pie chart above shows that this group of participants favoured content over technical clues with a ration of 56:43 (content:technical). In contrast, male participants showed no bias whatsoever with an even 50:50 split between both types, indicating that all elements of the emails were evaluated equally.

5.3.2.4. Comparison Results By Education

The comparison between highest and lowest scoring respondents by education level is shown in Figure 5-26 below.

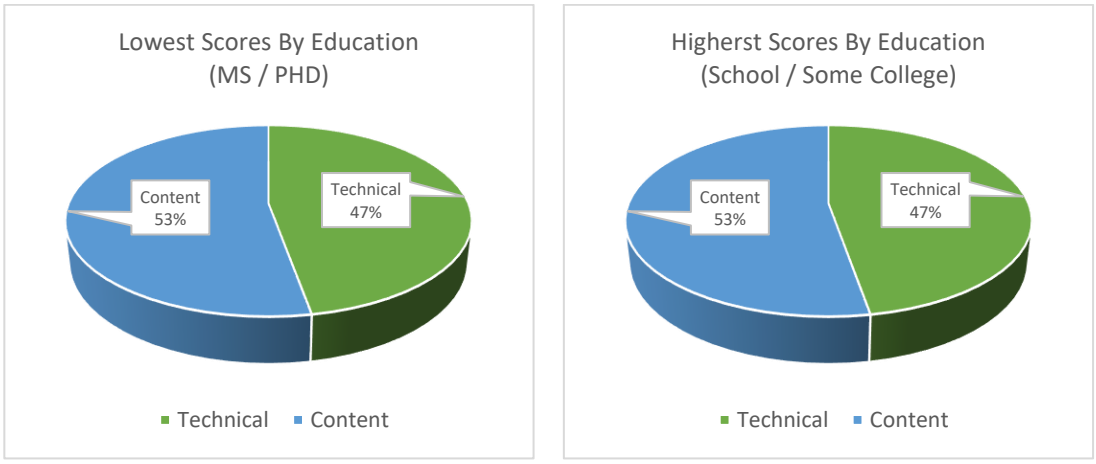


Figure 5-26 - Comparison Results By Education

In this example, both sets of respondents showed the same bias towards content within the test emails with a ration of 53:47 (content:technical) apparent in each group.

5.3.2.5. Comparison Results By Field of Work or Study

The comparison between highest and lowest scoring respondents by field of work or study is shown in Figure 5-27 below.

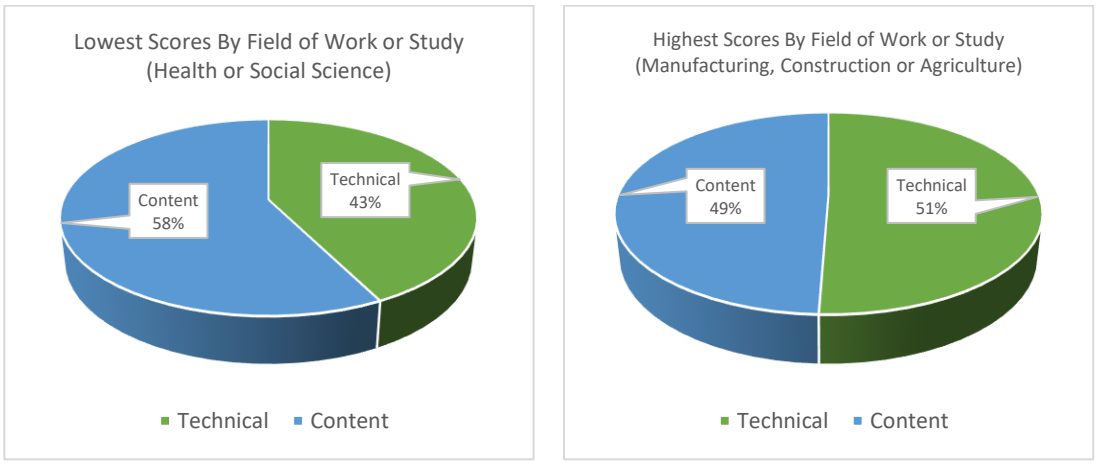


Figure 5-27 - Comparison By Field of Work Or Study

In this example, the lowest performers were those from a health or social science background and the highest performers were those with a background in manufacturing, construction or

agriculture. In this case, the lowest performers show a bias toward content with a ration of 58:42 (content:technical) across the test examples. In contrast, the best performers showed an almost unbiased ratio of 49:51 (content:technical) indicating that all elements of the emails were evaluated equally.

5.3.2.6. Comparison Results By Computer Literacy

The comparison between highest and lowest scoring respondents by computer literacy is shown in Figure 5-28 below.

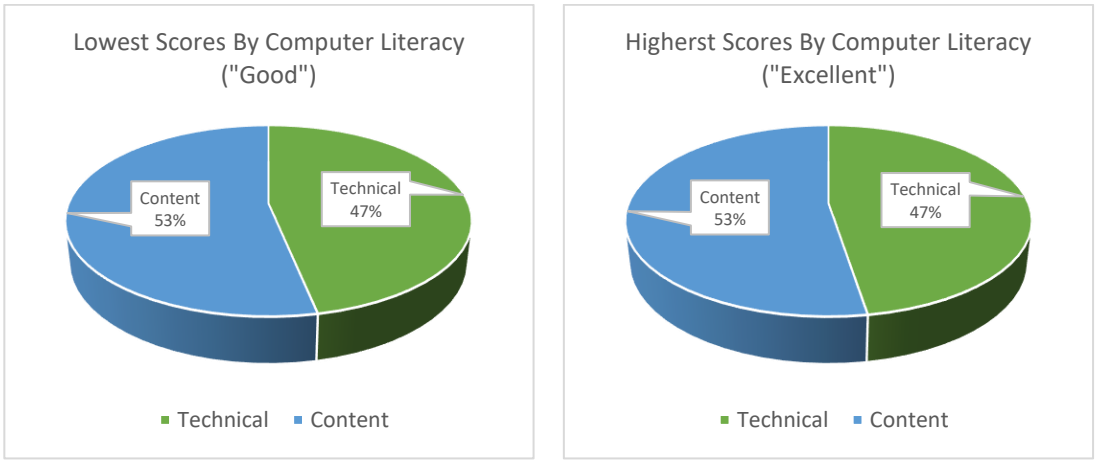


Figure 5-28 - Comparison Results By Computer Literacy

This example again shows the same results between each group of respondents with both sets of participants showing better rates of detection across content-focused examples at a ratio of 53:47 (content:technical)

5.3.2.7. Comparison Results By Expectation of Performance

The comparison between highest and lowest scoring respondents by performance expectation is shown in Figure 5-29 below.

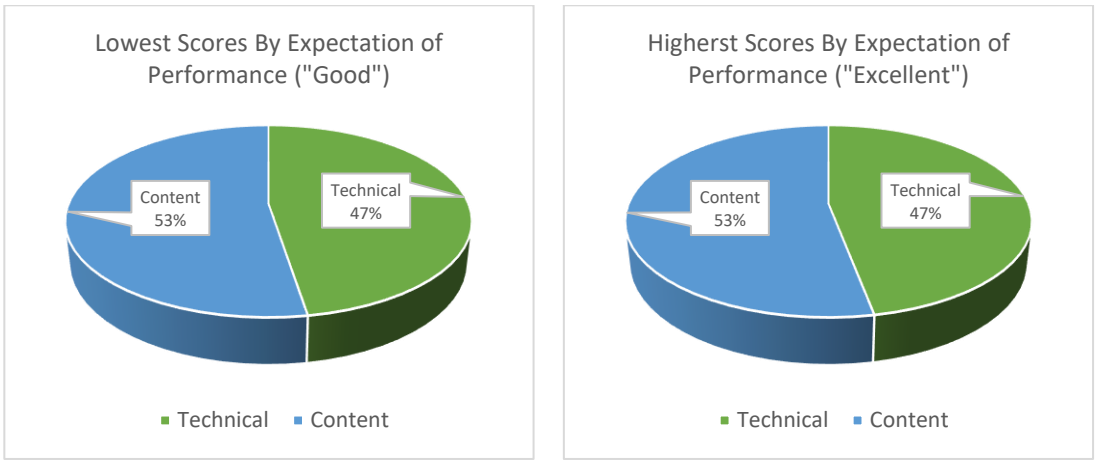


Figure 5-29 - Comparison Results By Expected Performance

Again, this example shows the same ratio of 53:47 (content:technical) across both sets of respondents exhibiting a slight bias towards content over technical clues in the test examples.

5.3.2.8. Comparison Results – Combined

The average of all of the previous results combined is shown in Figure 5-30 below, illustrating the average ratio of success across all groups between the technical and content-focused examples.

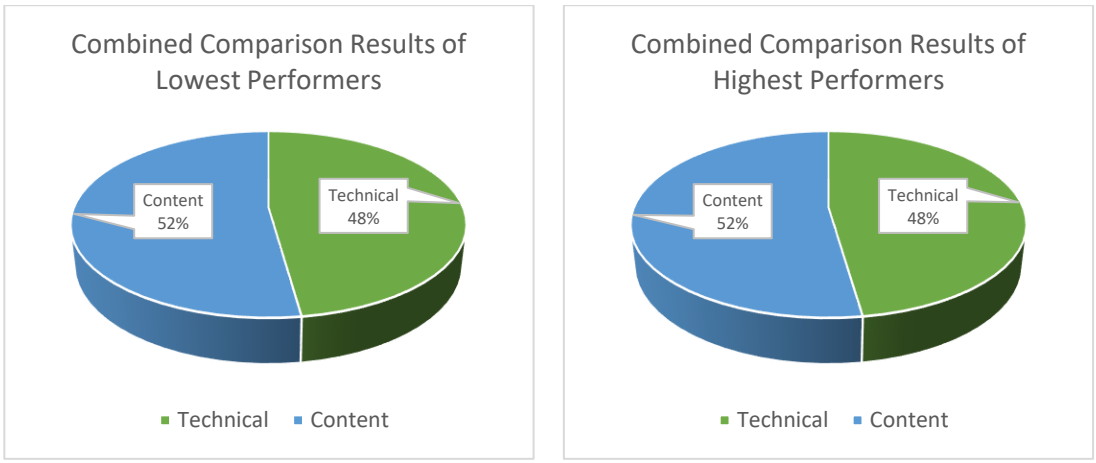


Figure 5-30 - Comparison Results - Combined

As the pie chart above illustrates, the overall performance across both groups. The best and worst performing are almost exactly the same, with both groups favouring content over technical elements by 52:48 (content:technical).

A 50:50 split would indicate that respondents were equally prone to technical deception and deception from within the content of the email and a result of 52:48 is statistically too close to that ratio to infer any statistical meaning.

5.4. Summary of Results & Analysis

This chapter has focused on the results of the phishing test as well as further analysis of how respondents may be processing information when deciding on the legitimacy of the test emails.

As discussed, in Section 4, the sample size was large with 217 complete responses and the distribution of respondents across the various groups (see section 4.3) consistently represented either a normal or approaching normal distribution across the sample. The results of the phishing test are summarised below.

5.4.1. Overall Results

The average score across the 217 participants was 66% with a median answer score of 70%. Out of the sample, only five respondents achieved a perfect score of 100%.

5.4.2. Demographics

Age: the study suggests that age may be a factor in susceptibility to phishing attacks with respondents in the "45-54" category performing the worst at 5% below average when the sample is adjusted to reflect the small number of respondents in the "18 – 24" and "64 – 74" categories.

Gender: the study suggests that gender may be a factor in susceptibility to phishing attacks with male respondents out-performing females, scoring 71% on average versus 62%. This figure would be greater if adjusted for sample size as female participants out-number males in the survey sample.

Education: an interesting finding from the study was that respondents with lower levels of education out-performed those with the highest education levels in the sample. Participants who reported their education level as "high school or equivalent" or "some college, no degree" performed between 8-10% better than average versus respondents with "masters degrees" or "PHD/doctorates" who performed 6-8% below average.

Field of Work or Study: respondents in the "manufacturing, construction or agriculture" categories were the best performers at 4% above average while respondents from the area of "health or social science performed the worst at 8% below average. An interesting finding is that respondents from the area of "business, other services, finance or insurance", who made up the largest part of the sample and who would be the category most exposed to email on a daily basis, performed at 2% below average across the test.

5.4.3. Experience

Experience of Online Services: the intention with this question was originally to see if respondents with experience of certain services, such as online shopping or banking, performed statistically better or worse than those unfamiliar with these services when presented with a fraudulent email from an organisation in that industry.

Unfortunately, most respondents reported familiarity with most of the services which made this comparison impossible. The study found, however, that respondents with a less than 40% success rate reported using 4 or less of these services versus the best performers who achieved a success rate of 80% or more who reported using 6 or more of them. Other secondary factors used as predictors of experience are discussed in the next section, however, they also failed to produce statistically significant results and overall the findings regarding the impact of experience on susceptibility to phishing were inconclusive.

5.4.4. Attitude to Privacy

Social Media Usage: there was some evidence that those with the largest social media footprint performed the worst in the test, the small sample size associated with these respondents makes it impossible to a infer statistically significant meaning from the result. The wider sample showed no significant difference in performance based on social media footprint.

Connections in Real Life: similarly, the number of connections reported by respondents known to them in real life proved inconclusive due to the high number of respondents who claimed to know all or most of their social media connections in that respect. While those who reported knowing the fewest of their social media connections in real life performed the worst, their sample size was again too small to offer statistically significant meaning from the results.

5.4.5. Self-Efficacy

Computer Literacy: respondents were asked to rate their computer literacy and perhaps unsurprisingly, those who self-identified as having excellent computer literacy outperformed all others with an average success rate of 70%.

Previous Training: an interesting finding of the study is that while almost half of the respondents reported previously receiving phishing awareness training, there was no statistical difference between either group of participants. This indicates that current training methods may not be effective in protecting individuals from phishing attacks.

Expectations of Success: respondents who expected excellent performance in the phishing test demonstrated that their self-confidence was well founded. Participants in this category outperforming all others with an average score of 7% above average.

5.4.6. Phishing Test Conclusion

In summary, the study produced evidence that factors such as demographics and self-efficacy may be a factor in an individual's susceptibility to phishing attacks. While previous studies have found that factors such as experience and attitude to privacy may also play a role, the findings from this study were inconclusive in these areas.

5.4.7. Summary of Further Investigation

Further investigation was undertaken on the preliminary findings to investigate if there was evidnece that respondents from the groups found to have statistically significant result were processing information differently when evaluating the legitimacy of the test examples.

The test scenarios were designed to feature either technical or content related indicators of legitimacy (or otherwise). A pattern of success or failure against either of these question types would indicate if respondents were relying on one type of indicator or the other when assessing the legitimacy of the test email examples. Should a pattern emerge, it could be concluded that respondents from different groups, in favouring one over the other, were processing the information presented to them within the email test examples in different ways. The exercise of designing each example is described in Section 3.3.4, and while some categories of participants showed clear performance differences in individual tests, most groups of respondents showed very little difference between the best and worst performers.

Overall, the sample was split 52:48 (content:technical) which is too close statistically from an even 50:50 split (no bias) to offer definitive insight into how information was processed by different groups of respondents during the test. The marginal lean towards content may indicate that participants rely more on the look and feel of an email when assessing its legitimacy and this is certainly an area that warrants further investigation. In addition, the consistent finding across all groups indicates that there may be no difference in how respondents process visual information when assessing emails for legitimacy.

6. Conclusions and Future Work

This section discusses the overall results of the study, including the definition of the problem and how it was address during the study. The expected results are discussed and compared to the actual findings of the research, along with the limiting factors relevant to the rusults. Finally, the contribution that this study makes to the existing body of research is discussed along with recommendations for further exploration and future work.

6.1. Research Overview

Phishing attacks are a modern-day confidence trick, where fraudsters target unsuspecting victims though seemingly genuine emails. The objective of a phishing attack is usually to deceive the recipient into revealing valuable private information and is usually financially-motivated. Phishing is on the rise, attackers are getting smarter, and the danger to individuals and organisations from these attacks is increasing. Phishing is also topical, with several high profile security breaches originating from phishing attacks in recent years. Moreover, while research has sought to understand who is likely to fall for a phishing attack, results to date have been inconclusive. The findings of different studies often contradict each other or the studies themselves were conducted too long ago. The Internet has never been so pervasive or its users so well informed but still phishing attacks continue to work. Previous research has shown that little is still known about why some users fall for a phishing attacks and some don't.

The goal of this study was twofold:

- First, the study sought to clarify what types of individuals were most perceptible to a phishing attack. The objective was to clarify what characteristics vulnerable people possessed, based on the factors previously established as indicators of susceptibility to phishing - demographics, experience, attitude to privacy and computer self-efficacy.
- The secondary goal of the study was to investigate if there was a pattern of behaviour apparent in the groups of respondents who performed the best and those who performed the worst in each category.

The phishing tests examples were designed to contain either technical deceptions or content related tricks. It was hoped that by comparing the success rate of the best and worst performers from each category, a pattern would emerge that might indicate that certain user types were more or less susceptible to either technical or content-based deception.

6.2. Problem Definition

The primary problem that this research set out to address was if different types of users, defined by demographics (age, gender, education, occupation, etc.), computer literacy (experience online, social networks, etc.) and attitudes to personal privacy perform better at identifying phishing attacks. The secondary objective was to assess how each respondent processed the visual clues in each test and to investigate if a pattern was apparent.

As such, the hypothesis (H1) was that there would be a statistically significant difference in the performance of different groups against phishing attacks. Also, it was expected that patterns of behaviour for each group would show a clear correlation between user type and how they assess information online.

The null hypothesis (H0) was that there would be no statistically significant difference between the defined groups regarding their effectiveness at detecting phishing scams.

6.3. Design/Experimentation, Results & Evaluation

6.3.1. Design / Experimentation

The study consisted of an online questionnaire and phishing test. Respondents were asked to anonymously answer ten questions about themselves and this information was used to segment respondents into the following categories:

- **Demographics:** Information such as age, gender, education and field of work or study. These are all metrics that have been identified in past research as statistically significant in relation to to susceptibility to phishing attacks.
- **Experience:** Online experience refers to the familiarity that the user has with online environments in general, and also the organisations or services that might be used in a spoof email. More experienced individuals are thought to be of lower risk, and the study attempted to test this from the perspective of both experience with specific online services and general experience of online environments overall.
- **Attitude to Privacy:** Previous research has shown users with a lower expectation of privacy, or a naïve trust in online environments, to be more susceptible to phishing. Using information regarding respondent's social media usage, the goal was first to prescribe a privacy score to participants and then compare their performance across the phishing tests.
- **Computer Self-Efficacy:** Lastly, it is well documented that an individual's confidence in their ability to effect a favourable outcome can positively affect the chances of them achieving that outcomes. As such the phenomenon of self-efficacy has been shown to be a factor in susceptibility to phishing attacks.

The phishing test portion of the study saw respondents asked to assess ten screenshots accompanied by a scenario. They were then asked if, in their opinion, each example was genuine or suspicious.The tests were presented to participants in a random order and consisted of three genuine emails and seven phishing emails. The tests were designed to present respondents with four examples of technical deception and four examples of content-based deception. In each case, three emails were spoofed, and one was real. In addition, two control emails were included - one genuine and one fake.

By designing the tests in such a way, it was hoped that a comparison could be made between the best and worst performers in each category to see if there was a pattern of detection across the technical or content-based tests. If there was evidence of a pattern, it could be inferred that different types of users were focusing on particular elements during the evaluation process. That, in turn, could infer that the way in which they were processing information online could be seen as a factor on their susceptibility to phishing.

6.3.2. Results

Analysis of the data was done in two parts. To begin, the overall performance of respondents was analysed to investigate if any group produced statistically significant results. These results are discussed below.

6.3.2.1. Demographics

The study indicates that age may be a factor in determining individuals susceptibility to phishing with respondents in the "45 – 54" category performed the worst. Previous studies have been inconsistent with regards to what age categories are most susceptible to phishing, however, this study supports the hypothesis that older internet users are most at risk from phishing scams.

Some studies have suggested that women are more susceptible to phishing attacks than men and this study supports that hypothesis with women averaging a score of 62% versus 71% for men.

Respondents with school or basic college outperformed better-educated participants with Masters or PhDs who were statistically the worst-performing group in the study. This supports the findings of previous studies that highly educated individuals can often perform badly in these scenarios, however, over-confidence, cited as a factor in some studies, does not appear to be an issue in this case as respondents who showed the highest level self-efficacy levels also performed the best. This finding may support the theory that lower educated individuals possess a higher level of overall distrust online. Another interesting finding is that participants from manufacturing, transport and agriculture, traditionally lower educated industries, outperformed all other respondents in the test. Further indicating that education level is not a contributing factor to success in detecting phishing scams.

6.3.2.2. Experience

The study was intended to assess if prior usage of a particular online service, such as online shopping, banking or media streaming etc. would impact on respondent's ability to assess test examples in that category correctly. Unfortunately, most respondents indicated prior use of practically all services making this impossible to assess. Secondary indicators of online experience also proved inconclusive, however, there was evidence that respondents with the lowest level of usage across these services also performed worse than those with higher usage statistics.

6.3.2.3. Attitude to Privacy

Assessing respondents attitudes to privacy also proved difficult for several reasons. Firstly, no statistically significant difference in performance could be attributed to respondent's social media footprint, a metric intended to indicate participants' expectation of privacy online. Secondly, almost all participants stated that they knew all or most of their online connections in real life, a metric intended to measure participants' level of trust in online environments. While some respondents stated that they knew only a few of their online connections in real life, and statistically performed worse than the rest of the sample, the number of participants in this group was too small to derive statistically significant meaning from the findings.

6.3.2.4. Computer Self-Efficacy

The study shows that participants who rated their computer literacy as "excellent", out-performed all other participants. Similarly, those that stated that they expected their performance in the test to be "excellent", also out-performed all other participants. Interestingly, there was no statistically significant difference between the performance of respondents who had previously received training and those who had not, indicating that existing methods of phishing awareness training may not be effective.

6.3.2.5. Summary of Further Investigation

Further investigation was undertaken on the preliminary findings to understand if respondents from statistically distinct groups were processing information in the test emails in different ways. While some categories of participants showed clear performance differences in individual tests, most groups showed very little difference between the best and worst performers. Overall, the sample was split 52:48 (content: technical) which is too close statistically from an even 50:50 split (no bias) to offer meaningful insight into how information was processed by different groups of respondents during the test. A ratio so close to 50:50 indicates that most participants assessed the test emails using a mix of both technical and non-techncial indicators of legitimacy.

6.3.2.6. Overview of Results

The primary goal of this research was to assess the accuracy with which different types of users, defined by demographics, experience online, attitudes to privacy and computer self-efficacy, could identify phishing attacks.

The hypothesis (H1) was that there would be a statistically significant difference in the performance of these groups. The findings from the study prove the hypothesis (H1) for respondents grouped by demographics and self-efficacy and are inconclusive with regards to online experience and attitudes to privacy.

The secondary objective was to assess how respondents processed the visual clues in each test and to investigate if this correlated with their grouping. In this instance, the null hypothesis (H0) was found to be true as the study showed no statistically significant difference between the defined groups regarding their patterns of detection. As such, it cannot be inferred if how participants process information online can be attributed as a factor in susceptibility to phishing attacks based on the findings of this study.

6.3.3. Evaluation & Reflection

The research has highlighted the complexity involved in assessing the vulnerability of individuals to phishing attacks. While many of the findings are in line with the existing body of research, that research is, itself, often contradictory. In addition, some of the findings from this study are somewhat counter-intuitive. One would expect that individuals with higher levels of education or employment in industries reliant on email for everyday tasks would perform the best, however, this was found not to be the case. It is interesting too that phishing awareness training appears to have had no significant impact on the performance of participants who had previously received it.

While the study met its primary objective, it is clear that the secondary objective was not adequately addressed. It may be that the way in which users process visual clues online is less of a factor in phishing susceptibility. It is more likely, however that the study employed an ineffective methodology in seeking to measure this metric. In addition, the desire to achieve a large sample size through the use of online platforms and social networks may have skewed the sample with under-representation of certain types of respondents, particularly in the younger and older age brackets.

6.4. Contributions To Body of Knowledge

While previous studies have investigated the factors that make individuals susceptible to phishing attacks, their findings have often been contradictory or inclusive. The findings of this study reinforce some of the findings from earlier studies and help to clarify further the demographic factors that can indicate susceptibility to phishing. Importantly, the study was performed at a time when phishing attacks are big news. In the wake of several high profile data breaches, the average email user is now more aware than ever of the dangers of online fraud. As such, the findings from the study become more relevant in the context of a group of participants who are likely more aware and more educated about the dangers and consequences of phishing attacks than those who have participated in previous studies.

While inconclusive, this study's attempt to measure how participants evaluate visual clues still holds merit. The study shows that phishing awareness training is broadly ineffective and without an understanding of how individuals process information online, and how it affects their decision making, it is difficult to see how this phenomenon can be successfully addressed.

Finally, the study's findings are significant because of the large and diverse sample of participants tested. Where previous studies have focused on specific populations, either by design or out of convenience, this study included over 200 participants, the large sample size achieved by leveraging the reach of social media and the topicality of the subject. As a result, the findings described in previous pages carry considerable weight.

6.5. Future Work and Recommendations

This study had two objectives. Firstly, it sought to investigate the performance of different types of individuals based on demographics, experience, attitude to privacy and computer self-efficacy. While the study presented clear findings regarding the role of demographics and self-efficacy as factors in phishing susceptibility, the results regarding experience and attitude to privacy were inconclusive.

Secondly, the study attempted to investigate if the way in which participants evaluated emails, based on technical and non-technical factors, was a factor in their susceptibility to phsihing attacks. These findings were also inclonclusive, indicating that most participants used both types of indicators when assessing the legitimacy of the email examples.

While many of the study's findings were inconclusive, it is clear that there is still no clear understanding of what makes an individual susceptible to phishing attacks. While it is emerging that certain categories of individuals are statistically more at risk than others, there is little evidence to suggest why. This is evidenced within this study where participants who had

previously received phishing awareness training performed on a par with those who had received none.

There were limiting factors withingthe design and execution of this study which, with the benefit of hindsight, could have been eliminated. In doing so, the findings may have been for conclusive. For example, the study focused on obtaining a large sample size, however it did not seek to ensure the relevance or diversity of the sample or align it with the necessary outputs of the research. In addition, the methodology employed to test how participants evaluated the email examples may not have been appropriate. Performing a similar study with a more balanced sample and a more accurate mechanism for measuring how respondents' process visual information would undoubtedly yield better results.

In summary, future work should focus on truly understanding what cognative factors make individuals susceptible to phishing. While it is useful to understand that users with certain socio-economic backgrounds are more at risk than others, it is only half the story. Based on the findings of this study, the obvious next step would be to repeat the study with a more representative sample while devising a more accurate testing mechanism, that maintains the convenience and light cognitive load of this study.

7. Bibliography

Alghamdi, H. (2017). *Can Phishing Education Enable Users To Recognise Phishing Attacks?* Dublin Institute of Technology, School of Computing.

Alqarni, Z., Algarni, A., & Xu, Y. (2016). Toward Predicting Susceptibility to Phishing Victimization on Facebook (pp. 419–426). Presented at the 2016 IEEE International Conference on Services Computing (SCC), IEEE.

Alseadoon, I., Chan, T., Foo, E., & Gonzales Nieto, J. (2012). Who is more susceptible to phishing emails?: a Saudi Arabian study. In *ACIS 2012: Location, location, location: Proceedings of the 23rd Australasian Conference on Information Systems 2012* (pp. 1–11). ACIS.

Anandpara, V., Dingman, A., Jakobsson, M., Liu, D., & Roinestad, H. (2007). Phishing IQ Tests Measure Fear, Not Ability. In S. Dietrich & R. Dhamija (Eds.), *Financial Cryptography and Data Security* (Vol. 4886, pp. 362–366). Berlin, Heidelberg: Springer Berlin Heidelberg.

Anderson, B., Vance, A., & Eargle, D. (2013). Is Your Susceptibility to Phishing Dependent on Your Memory. In *Proceedings of the Eighth Pre-ICIS Workshop on Information Security and Privacy* (Vol. 1).

Ang, L., Dubelaar, C., & Lee, B.-C. (n.d.). To Trust or Not to Trust? A Model of Internet Trust from the Customer's Point of View, 13.

Anti-Phishing Working Group. (2017). *Phishing Activity Trends Report, 3rd Quarter 2017* (p. 13).

Arachchilage, N. A. G., & Love, S. (2014). Security awareness of computer users: A phishing threat avoidance perspective. *Computers in Human Behavior*, *38*, 304–312.

Ariguzo, G. C., Mallach, E. G., & White, D. S. (2006). The first decade of e-commerce, *1*(3), 17.

Association for Computing Machinery, Special Interest Group on Computer and Human Interaction, New Zealand Chapter, CHI 2017, & Annual CHI Conference on Human Factors in Computing Systems. (2016). *CHI'17 Proceedings of the 2017 ACM SIGCHI Conference on Human Factors in Computing Systems, May 6-11, 2017, Denver, CO, USA*. New York, NY: ACM.

Banu, N., & Banu, S. M. (2013). A Comprehensive Study of Phishing Attacks. *International Journal of Computer Science and Information Technologies*, *4*(6).

Becker, R. A., Volinsky, C., & Wilks, A. R. (2010). Fraud Detection in Telecommunications: History and Lessons Learned. *Technometrics*, *52*(1), 20–33.

Berners-Lee, T., & Fischetti, M. (2001). *Weaving the Web: The Original Design and Ultimate Destiny of the World Wide Web by Its Inventor*. DIANE Publishing Company.

Berners-Lee, T., Hendler, J., & Lassila, O. (2001). Scientific American: Feature Article: The Semantic Web: May 2001. *Scientific American*, 4.

Blomqvist, K. (1997a). The many faces of trust. *Scandinavian Journal of Management*, *13*(3), 271–286.

Button, M., Nicholls, C. M., Kerr, J., & Owen, R. (2016). Online frauds: Learning from victims why they fall for these scams. *Australian & New Zealand Journal of Criminology*, *18*.

Castells, M. (2002). *The Internet Galaxy: Reflections on the Internet, Business, and Society*. OUP Oxford.

Chakraborty, R., Vishik, C., & Rao, H. R. (2013). Privacy-preserving actions of older adults on social media: Exploring the behaviour of opting out of information sharing. *Decision Support Systems*, *55*(4), 948–956.

Chandrasekaran, M., Chinchani, R., & Upadhyaya, S. (2006). Phoney: Mimicking user response to detecting phishing attacks. In *Proceedings of the 2006 International Symposium on World of Wireless, Mobile and Multimedia Networks* (pp. 668–672). IEEE Computer Society.

Chandrasekaran, M., Narayanan, K., & Upadhyaya, S. (2006). Phishing E-mail Detection Based on Structural Properties. In *Proceedings of 9th Annual NYS Cyber Security Conference* (p. 7). Albany, NY.

Chin, E., Porter, A., Kate, F., & Wagner, G. D. (2011). Analyzing Inter-Application Communication in Android. In *InProceedings of the 9thAnnual International Conference onMobile Systems, Applications, and Services, MobiSys*.

Chung, J. E., Park, N., Wang, H., Fulk, J., & McLaughlin, M. (2010). Age differences in perceptions of online community participation among non-users: An extension of the Technology Acceptance Model. *Computers in Human Behavior*, *26*(6), 1674–1684.

Clark, A., Adams, B., & Craven, J. (2018). It is Free and Always Will Be (p. 15). Presented at the Convenience of Online Services.

Dean, D., Felten, E. W., & Wallach, D. S. (1996). Java security: From HotJava to Netscape and beyond (pp. 190–200). IEEE Comput. Soc. Press.

Debatin, B., Lovejoy, J. P., Horn, A.-K., & Hughes, B. N. (2009). Facebook and Online Privacy: Attitudes, Behaviors, and Unintended Consequences. *Journal of Computer-Mediated Communication*, *15*(1), 83–108.

Dhamija, R., Tygar, J. D., & Hearst, M. (2006). Why phishing works. In *Proceedings of the SIGCHI conference on Human Factors in computing systems* (pp. 581–590). ACM.

Dickson, G. W., & Simmons, J. K. (1970). The behavioural side of MIS Some aspects of the "people problem". *Business Horizons*, *13*(4), 59–71.

Dinev, T., & Hart, P. (2006). An Extended Privacy Calculus Model for E-Commerce Transactions. *Information Systems Research*, *17*(1), 61–80.

Downs, J. S., Holbrook, M. B., & Cranor, L. F. (2006). Decision strategies and susceptibility to phishing (p. 79). ACM Press.

Downs, J. S., Holbrook, M., & Cranor, L. F. (2007). Behavioural response to phishing risk. In *Proceedings of the anti-phishing working groups 2nd annual eCrime researchers summit* (pp. 37–44). ACM.

Ehrenfeld, J. M. (2017). WannaCry, Cybersecurity and Health Information Technology: A Time to Act. *Journal of Medical Systems*, *41*(7), 104.

Eisend, M., & Schuchert-güler, P. (2006). Explaining Counterfeit Purchases: A Review and Preview. *Academy of Marketing Science Review*, *2006*(12).

El-Din, R. S. (2012). To deceive or not to deceive! Ethical questions in phishing research. In *HCI Research in Sensitive Contexts: Ethical Considerations Workshop at HCI* (pp. 10–14).

Eveland, W. P., & Dunwoody, S. (2001). User Control and Structural Isomorphism or Disorientation and Cognitive Load?: Learning From the Web Versus Print. *Communication Research*, *28*(1), 48–78.

Fogg, B., Marshall, J., Laraki, O., Osipovich, A., Varma, C., Fang, N., … Treinen, M. (2001). *anyone. anywhere. What Makes Web Sites Credible? A Report on a Large Quantitative Study*.

Fogg, B., Soohoo, C., Danielson, D., Marable, L., Stanford, J., & Tauber, E. R. (2002). How Do People Evaluate a Web Site's Credibility? *Stanford Guidelines for Web Credibility*, 105.

Found, B. (2015). Deciphering the human condition: the rise of cognitive forensics. *Australian Journal of Forensic Sciences*, *47*(4), 386–401.

Gandy, O. H. (1993). *The Panoptic Sort: A Political Economy of Personal Information. Critical Studies in Communication and in the Cultural Industries*. Westview Press, Inc.

Gefen, Karahanna, & Straub. (2003). Trust and TAM in Online Shopping: An Integrated Model. *MIS Quarterly*, *27*(1), 51.

Gerbaudo, P. (2018). *Tweets and the Streets : Social Media and Contemporary Activism*. Pluto Press. Retrieved from

Grabner-Kraeuter, S. (2002). The role of consumers' trust in online shopping. *Journal of Business Ethics*, *39*(1–2), 43–50.

Gutenberg, P., & Hart, M. (n.d.). Hobbes' Internet Timeline - the definitive ARPAnet & Internet history, 34.

Hong, J. (2012). The Current State of Phishing Attacks. *Communications of the ACM*, *55*(1), 74–81.

Hoofnagle, C. J., King, J., Li, S., & Turow, J. (2010). How Different are Young Adults from Older Adults When it Comes to Information Privacy Attitudes and Policies? *SSRN Electronic Journal*.

Iuga, C., Nurse, J. R. C., & Erola, A. (2016). Baiting the hook: factors impacting susceptibility to phishing attacks. *Human-Centric Computing and Information Sciences*, *6*(1).

Jansen, J., & Leukfeldt, R. (2016). Phishing and malware attacks on online banking customers in the Netherlands: A qualitative analysis of factors leading to victimization. *International Journal of Cyber Criminology*, *10*(1), 79.

Jasper, S. (2017). Russia and Ransomware: Stop the Act, Not the Actor. *Calhoun: The NPS Institutional Archive*, 4.

Katz, J. E., Rice, R. E., & Aspden, P. (2001). The Internet, 1995-2000: Access, Civic Involvement, and Social Interaction. *American Behavioral Scientist*, *45*(3), 405–419.

Kelley, C. M., Hong, K. W., Mayhorn, C. B., & Murphy-Hill, E. (2012). Something smells phishy: Exploring definitions, consequences, and reactions to phishing. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* (Vol. 56, pp. 2108–2112). SAGE Publications Sage CA: Los Angeles, CA.

Kim, B.-K. (2005). *Internationalizing the Internet: The Co-evolution of Influence and Technology*. Edward Elgar Publishing.

Kirwan, D. (2017). *Cybercrime: An Investigation of the Attitudes and Environmental Factors that Make People more Willing to Participate in Online Crime*. Dublin Institute of Technology, Dublin, Ireland.

Kumaraguru, P., Cranshaw, J., Acquisti, A., Cranor, L., Hong, J., Blair, M. A., & Pham, T. (2009). School of Phish: A Real-World Evaluation of Anti-Phishing Training (p. 12). Presented at the Symposium on Usable Privacy and Security, Mountainview, CA.

Langenderfer, J., & Shimp, T. A. (2001). Consumer vulnerability to scams, swindles, and fraud: A new theory of visceral influences on persuasion. *Psychology & Marketing*, *18*(7), 763–783.

Leiner, B. M., Cerf, V. G., Clark, D. D., Kahn, R. E., Kleinrock, L., Lynch, D. C., … Wolff, S. (2009). Brief History of the Internet - Internet Timeline | Internet Society. *ACM SIGCOMM Computer Communication Review*, *39*(5), 9.

Mace, M. (2010). Browsing as the killer app: Explaining the rapid success of Apple's iPhone. *Telecommunications Policy*, 270–286.

Miltgen, C. L., & Peyrat-Guillard, D. (2014). Cultural and generational influences on privacy concerns: a qualitative study in seven European countries. *European Journal of Information Systems*, *23*(2), 103–125.

Parsons, K., McCormac, A., Butavicius, M., & Ferguson, L. (2010, October). Human Factors and Information Security: Individual, Culture and Security Environment. Command, Control, Communications and Intelligence Division.

Parsons, K., McCormac, A., Pattinson, M., Butavicius, M., & Jerram, C. (2013). Phishing for the truth: A scenario-based experiment of users' behavioural response to emails. In *IFIP International Information Security Conference* (pp. 366–378). Springer.

Rajivan, P., & Gonzalez, C. (2018). Creative Persuasion: A Study on Adversarial Behaviors and Strategies in Phishing Attacks. *Frontiers in Psychology*, *9*.

Resnick, P., Zeckhauser, R., Friedman, E., & Kuwabara, K. (n.d.). For buyers and sellers alike, there's no better way to earn one another's trust in online interactions. *COMMUNICATIONS OF THE ACM*, *43*(12), 4.

Rodgers, S., & Thorson, E. (2000). The Interactive Advertising Model: How Users Perceive and Process Online Ads. *Journal of Interactive Advertising*, *1*(1), 41–60.

Ryan, M.-L. (2001). *Narrative as virtual reality: immersion and interactivity in literature and electronic media*. Baltimore: Johns Hopkins University Press.

Salus, P. H. (1995). *Casting the Net: From ARPANET to Internet and Beyond...* Boston, MA, USA: Addison-Wesley Longman Publishing Co., Inc.

Sheehan, K. B. (2002). Toward a typology of Internet users and online privacy concerns. *The Information Society*, *18*(1), 21–32.

Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L. F., & Downs, J. (2010). Who falls for phish?: a demographic analysis of phishing susceptibility and effectiveness of interventions. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 373–382). ACM.

Silic, M., & Back, A. (2016). The dark side of social networking sites:Understanding phishing risks. *Computers in Human Behavior*, *60*, 35–43.

Stajano, F., & Wilson, P. (2011). Understanding scam victims: seven principles for systems security. *Communications of the ACM*, *54*(3), 70.

Stavroulakis, P., & Stamp, M. (Eds.). (2013). Phishing: A Computer Security Threat. *International Journal of Advanced Research in Computer Science and Management Studies*, *1*(1), 64–71.

Tembe, R., Hong, K. W., Murphy-Hill, E., Mayhorn, C. B., & Kelley, C. M. (2013). American and Indian conceptualisations of phishing. In *Socio-Technical Aspects in Security and Trust (STAST), 2013 Third Workshop on* (pp. 37–45). IEEE.

van Dijk, J., & Hacker, K. (2003). The Digital Divide as a Complex and Dynamic Phenomenon. *The Information Society*, *19*(4), 315–326.

Vishwanath, A. (2015). Habitual Facebook Use and its Impact on Getting Deceived on Social Media. *Journal of Computer-Mediated Communication*, *20*(1), 83–98.

Vishwanath, A., Herath, T., Chen, R., Wang, J., & Rao, H. R. (2011). Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model. *Decision Support Systems*, *51*(3), 576–586.

Vue, S., Student, U., Schmidt, M., & Price, E. (2013). *GONE PHISHING: SURVEYING COLLEGE STUDENTS ON PHISHING AWARENESS AND COMPETENCY*. St. Cloud State University, St. Cloud, MN 56301.

Wang, J., Li, Y., & Rao, H. R. (2016). Overconfidence in Phishing Email Detection. *Journal of the Association for Information Systems*, *17*(11).

Wardrip-Fruin, N. (2004). What hypertext is (p. 126). ACM Press.

Wright, R. T., & Marett, K. (2010). The Influence of Experiential and Dispositional Factors in Phishing: An Empirical Investigation of the Deceived. *Journal of Management Information Systems*, *27*(1), 273–303.

Wu, M., Miller, R. C., & Garfinkel, S. L. (2006). Do security toolbars actually prevent phishing attacks? (p. 601). ACM Press.

Zhang, Y., Egelman, S., Cranor, L., & Hong, J. (2006). *Phinding Phish: Evaluating anti-phishing tools*. Carnegie Mellon University, Human-Computer Interaction Institute.

Appendix 1 – Questionairre

Real or Fake - can you tell the difference?

Introduction

Hello.

I am conducting research on email security as part of my dissertation for my masters degree in computer science.

The study comprises of 2 sections - a short questionnaire of 10 questions followed by a short test. Please answer truthfully. Please complete all questions. It should take no more than 5 - 10 minutes.

Participation in this study is completely anonymous and the information collected through this research will not be used by any third party.

This study is compliant with general data protection legislation (GDPR).

Thank you for your participation.

Charlie

Real or Fake - can you tell the difference?

Section 1 - Questionnaire

Instructions:

In this section, you will be asked to complete a short questionnaire. Please answer truthfully. You must answer all questions and all answers are anonymous.

* 1. What is your age?

- ○ Under 18
- ○ 18 to 24
- ○ 25 to 34
- ○ 35 to 44
- ○ 45 to 54
- ○ 55 to 64
- ○ 65 to 74
- ○ 75 or older

* 2. What is your gender?

- ○ Male
- ○ Female

* 3. What is the highest level of education you have completed?

[ ]

* 4. Which of the following best describes the industry within which you work or are studying?

- ○ Transport, retail or wholesale
- ○ Business and other services, finance or insurance
- ○ Manufacturing, construction or agriculture
- ○ Hospitality, catering or leisure services
- ○ Health or social science
- ○ Public sector or education
- ○ None of the above

* 5. Have you ever used any of these products or services online? (please select all that apply)

- ☐ Online banking or payment services
- ☐ Online shopping
- ☐ Video streaming / entertainment services
- ☐ Courier / parcel delivery services
- ☐ Home or car insurance
- ☐ Social media networks
- ☐ None of the above

* 6. Which of these social media networking sites do you currently have an account with? (please select all that apply)

- [ ] Facebook
- [ ] Google+
- [ ] Instagram
- [ ] Twitter
- [ ] LinkedIn
- [ ] Snapchat
- [ ] Tumblr
- [ ] Reddit
- [ ] Pinterest
- [ ] Foursquare
- [ ] Ravelry
- [ ] Yourtube
- [ ] Flickr
- [ ] Qzone
- [ ] Weibo
- [ ] Ask.fm
- [ ] VK
- [ ] Odnoklassniki
- [ ] Meetup
- [ ] None of these

* 7. About how many of your friends / connections on social networking services have you met in person?

- ( ) All of them
- ( ) Most of them
- ( ) About half of them
- ( ) A few of them
- ( ) None of them

* 8. How would you describe your computer literacy?

- ( ) Excellent
- ( ) Good
- ( ) Neither good or bad
- ( ) Bad
- ( ) Terrible

* 9. Have you ever received training about how to spot a suspicious email?

- ( ) Yes
- ( ) No
- ( ) Other (please specify)

* 10. How good would you expect to be at identifying a suspicious email?

- ( ) Excellent
- ( ) Good
- ( ) Neither good or bad
- ( ) Bad
- ( ) Terrible

Appendix 2 – Phishing Test

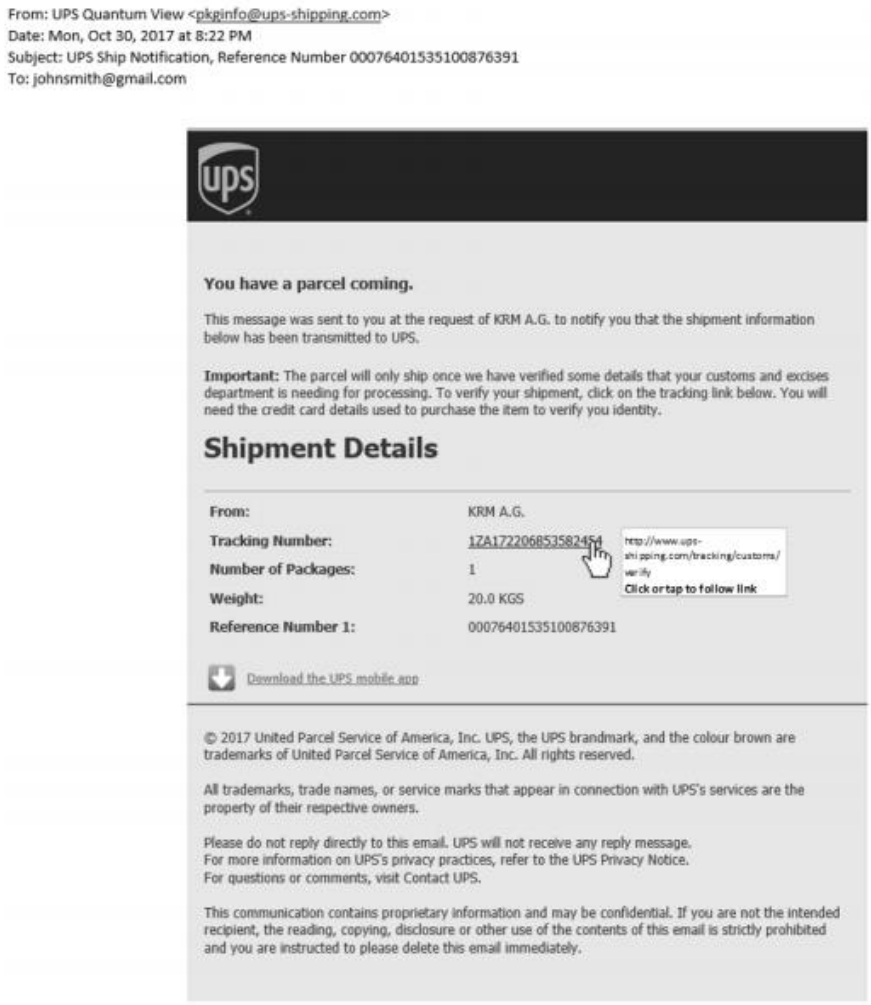
Real or Fake - can you tell the difference?

Section 2 - The Test

Instructions:

In this section you will be shown 10 emails along with a short paragraph describing the circumstances under which they were received. It is your job to decide if the email seems genuine or suspicious. If you are unsure, please select "don't know".

* 11. You buy a lot of goods online and regularly receive notifications of parcels being shipped to you. While you cannot remember this particular order, it's not unusual for you to receive these notifications and not remember the transaction.



From: UPS Quantum View <pkginfo@ups-shipping.com>
Date: Mon, Oct 30, 2017 at 8:22 PM
Subject: UPS Ship Notification, Reference Number 00076401535100876391
To: johnsmith@gmail.com

You have a parcel coming.

This message was sent to you at the request of KRM A.G. to notify you that the shipment information below has been transmitted to UPS.

Important: The parcel will only ship once we have verified some details that your customs and excises department is needing for processing. To verify your shipment, click on the tracking link below. You will need the credit card details used to purchase the item to verify you identity.

Shipment Details

From:	KRM A.G.
Tracking Number:	1ZA172206853582454
Number of Packages:	1
Weight:	20.0 KGS
Reference Number 1:	00076401535100876391

http://www.ups-shipping.com/tracking/customs/verify
Click or tap to follow link

Download the UPS mobile app

Please do not reply directly to this email. UPS will not receive any reply message.
For more information on UPS's privacy practices, refer to the UPS Privacy Notice.
For questions or comments, visit Contact UPS.

Does this email seem genuine or suspicious?

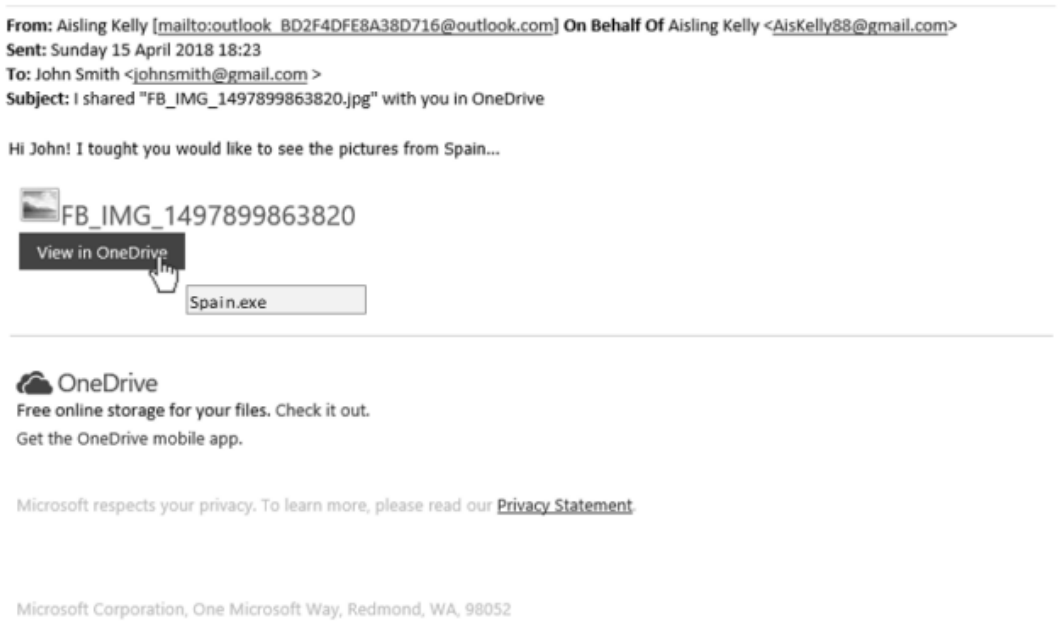
- ◯ Genuine
- ◯ Suspicious
- ◯ I am not sure

* 12. You receive an email from 123.ie confirming the renewal of your home insurance policy and providing documents relevant to your cover. You have had your home insurance with 123.ie for the past few years and recently completed the renewal process over the phone with an operator called Mary.

Does this email seem genuine or suspicious?

- ◯ Genuine
- ◯ Suspicious
- ◯ I am not sure

* 13. You receive an email from your friend Aisling who you went to college with. Aisling wants to share some pictures with you from her recent tripto Spain using Microsoft OneDrive



From: Aisling Kelly [mailto:outlook_BD2F4DFE8A38D716@outlook.com] **On Behalf Of** Aisling Kelly <AisKelly88@gmail.com>
Sent: Sunday 15 April 2018 18:23
To: John Smith <johnsmith@gmail.com >
Subject: I shared "FB_IMG_1497899863820.jpg" with you in OneDrive

Hi John! I tought you would like to see the pictures from Spain...

FB_IMG_1497899863820

View in OneDrive

Spain.exe

OneDrive
Free online storage for your files. Check it out.
Get the OneDrive mobile app.

Microsoft respects your privacy. To learn more, please read our Privacy Statement.

Microsoft Corporation, One Microsoft Way, Redmond, WA, 98052

Does this email seem genuine or suspicious?

- ○ Genuine
- ○ Suspicious
- ○ I am not sure

* 14. You are an active Facebook user, regularly logging in from different devices, and you receive the email below

From: Facebook <omar1991@hotmail.com>
Date: Tue, Mar 20, 2018 at 6:29 PM
Subject: Facbook Security Alert – Urgent Action Require!
To: John Smith <johnsmith@gmail.com>

—

Security Alert from Facebook

Hello Facebook Member,

The Facebook account associated with you email address had too many wrong username and password attempt. Your account is locked and will be deleted if you do not login again and fix this problem soon.

Please visit the Security Centre to reactivate the account.

Faceebook, Inc., Attention: Community Se 4025

info@cwfbqwazlov3yp7kjxcwfbqwazlov3yp7kjx-------.ec2-54-69-89-15.us-west-2.compute.amazonaws.com
Click or tap to follow link

Does this email seem genuine or suspicious?

- ○ Genuine
- ○ Suspicious
- ○ I am not sure

* 15. Getting goods shipped to Ireland can be a pain so you often use Parcel Motel, a courier forwarding service, to get cheap shipping from the UK. You receive the below email informing you that you have insufficient funds for your latest delivery which you suspect is that order you placed a few days ago.

From: Parcel Motel Check In <parcelmotel@circulator.com>
Date: Tue, Apr 10, 2018 at 7:25 PM
Subject: Insufficient Funds
To: <johnsmith@gmail.com>

Click here to view this email online »

PARCELMOTEL.COM

SIGN IN

Hi John Smith

Your parcel has arrived at our Dublin Depot but you have insufficient funds in your account to cover the €3.95 to receive your parcel. It may be that your credit card has expired.

Please **log in** to your Parcel Motel account in order to top up. Once you have completed this process, no further action is required as your parcel will automatically be released for delivery.

SIGN IN

Why not avail of our €35 Top

If you top up by €35 in a single payment we will add €4.50 to your account*

*You must top up by €35 at a time to avail of this offer. The bonus will be applied as credit to your Parcel Motel account. No cash alternative or refunds are applicable.

Kind regards,

The Parcel Motel Team

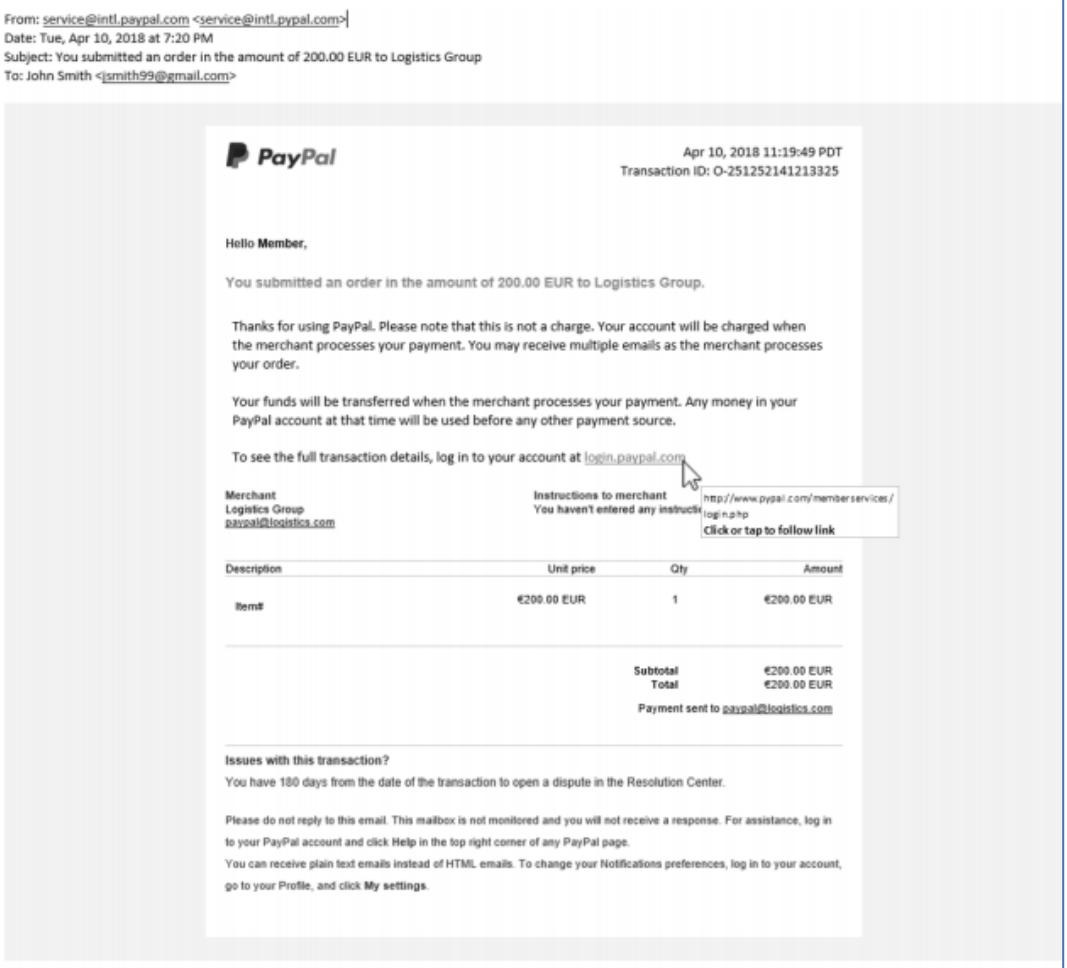
You are receiving this email as a registered Parcel Motel member.

Terms & Conditions Privacy Policy Support Returns Shop © Parcel Motel 2015 Nightline

Does this email seen genuine or suspicious?

- Genuine
- Suspicious
- I am not sure

* 16. You receive an email from PayPal, who you use a lot to pay for things online. The email is a notification that you have paid a sum of money to a receiver you do not recognize or remember. This has happened in the past when the business name has been different from the trading name.



From: service@intl.paypal.com <service@intl.pypal.com>
Date: Tue, Apr 10, 2018 at 7:20 PM
Subject: You submitted an order in the amount of 200.00 EUR to Logistics Group
To: John Smith <jsmith99@gmail.com>

PayPal

Apr 10, 2018 11:19:49 PDT
Transaction ID: O-251252141213325

Hello **Member**,

You submitted an order in the amount of 200.00 EUR to Logistics Group.

Thanks for using PayPal. Please note that this is not a charge. Your account will be charged when the merchant processes your payment. You may receive multiple emails as the merchant processes your order.

Your funds will be transferred when the merchant processes your payment. Any money in your PayPal account at that time will be used before any other payment source.

To see the full transaction details, log in to your account at login.paypal.com

Merchant
Logistics Group
paypal@logistics.com

Instructions to merchant
You haven't entered any instructi

http://www.pypal.com/memberservices/login.php
Click or tap to follow link

Description	Unit price	Qty	Amount
Item#	€200.00 EUR	1	€200.00 EUR

Subtotal €200.00 EUR
Total €200.00 EUR

Payment sent to paypal@logistics.com

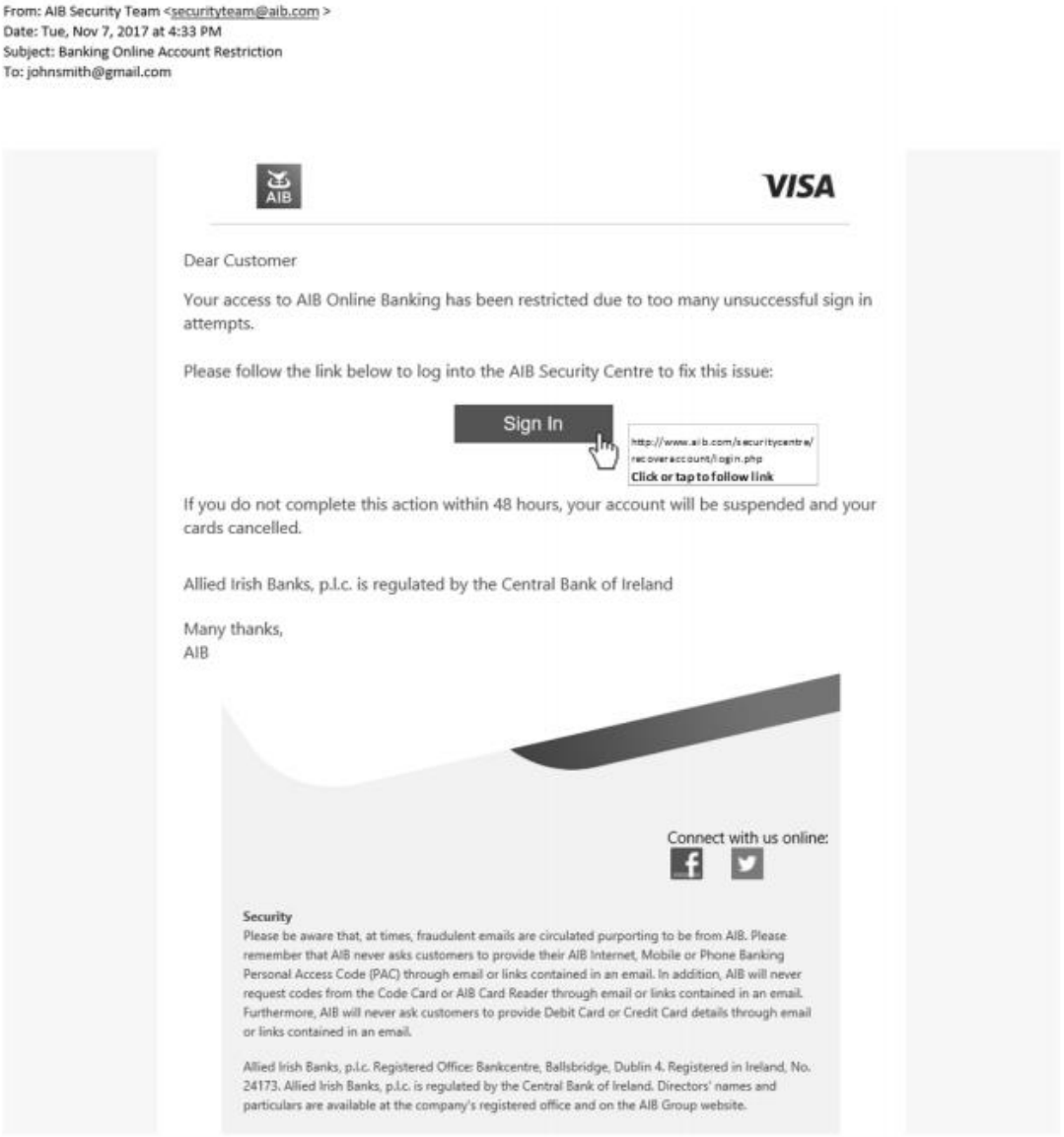
Issues with this transaction?
You have 180 days from the date of the transaction to open a dispute in the Resolution Center.

Please do not reply to this email. This mailbox is not monitored and you will not receive a response. For assistance, log in to your PayPal account and click **Help** in the top right corner of any PayPal page.
You can receive plain text emails instead of HTML emails. To change your Notifications preferences, log in to your account, go to your Profile, and click **My settings**.

Does this email seem genuine or suspicious?

- ◯ Genuine
- ◯ Suspicious
- ◯ I am not sure

* 17. Your bank (AIB) emails you to alert you to suspicious activity on you online banking facility. You have been an AIB customer for years and use the online banking facility regularly



From: AIB Security Team <securityteam@aib.com >
Date: Tue, Nov 7, 2017 at 4:33 PM
Subject: Banking Online Account Restriction
To: johnsmith@gmail.com

AIB VISA

Dear Customer

Your access to AIB Online Banking has been restricted due to too many unsuccessful sign in attempts.

Please follow the link below to log into the AIB Security Centre to fix this issue:

Sign In

http://www.aib.com/securitycentre/recoveraccount/login.php
Click or tap to follow link

If you do not complete this action within 48 hours, your account will be suspended and your cards cancelled.

Allied Irish Banks, p.l.c. is regulated by the Central Bank of Ireland

Many thanks,
AIB

Connect with us online:

Security
Please be aware that, at times, fraudulent emails are circulated purporting to be from AIB. Please remember that AIB never asks customers to provide their AIB Internet, Mobile or Phone Banking Personal Access Code (PAC) through email or links contained in an email. In addition, AIB will never request codes from the Code Card or AIB Card Reader through email or links contained in an email. Furthermore, AIB will never ask customers to provide Debit Card or Credit Card details through email or links contained in an email.

Allied Irish Banks, p.l.c. Registered Office: Bankcentre, Ballsbridge, Dublin 4. Registered in Ireland, No. 24173. Allied Irish Banks, p.l.c. is regulated by the Central Bank of Ireland. Directors' names and particulars are available at the company's registered office and on the AIB Group website.

Does this email seem genuine or suspicious?

- ◯ Genuine
- ◯ Suspicious
- ◯ I am not sure

* 18. As an Amazon customer, you receive emails from them all the time with various offers and promotions or to inform you of changes to the site.

From: Amazon.co.uk <amazon.co.uk@amazonservices.de >
Date: Wed, Apr 11, 2018 at 1:26 AM
Subject: Response required
To: johnsmith@gmail.com

amazon.co.uk prime

Hello,

Due to a recent upgrade of our servers, we have urged all our shopping users for possible account re-verification. For your protection, make sure you verify your Amazon account before someone might attempt to access your account.

Kindly log into your account at www.amazon.co.uk to verify your personal and payment details.

http://www.amazonservices.de/secure/homepage.html/ref=nav_youraccount_btn
Click or tap to follow link

We are working to make sure all our customers accounts is as safe and secured. We apologise for any inconvenience and thank you for your prompt attention in this matters.

We hope to see you again soon.
Amazon.co.uk

Top Picks for You

Play and Charge Kit Plus - Microsoft Officially...
£14.99

Seagate 2 TB FireCuda 2.5 Inch Internal SSHD...
£79.72

Crucial CT1050MX300SSD1 MX300 1 TB 3D NAND SATA...
£203.00

Amazon EU société à responsabilité limitée, 5 rue Plaetis, L-2338 Luxembourg. Share capital: EUR 37,500. RCS Luxembourg Number: B 101818. Business License Number: 134248. Luxembourg VAT Registration Number: LU 20260743.

Learn more about your statutory rights here.

Please note: This email was sent from a notification-only address that can't accept incoming email. Please do not reply to this message.

Does this email seem genuine or suspicious?

- ○ Genuine
- ○ Suspicious
- ○ I am not sure

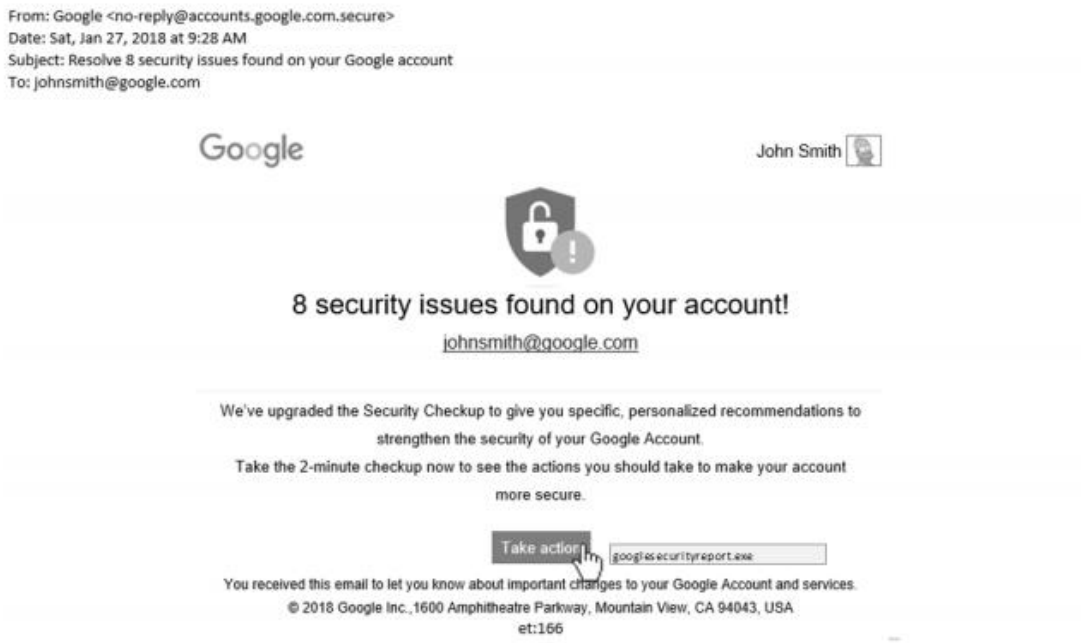
* 19. Netflix, who you use regularly to stream movies and TV shows, emails you to inform you of some changes made to your account

Does this email seem genuine or suspicious?

- ◯ Genuine
- ◯ Suspicious
- ◯ I am not sure

* 20. Google is your email provider through their Gmail service and you also use your Google credentials on your Android phone, Google Maps, YouTube and several other websites. Your email address is "johnsmith@google.com" and you use a picture of Homer Simpson as your public profile pic on Google+

You receive the below security report from Google


From: Google <no-reply@accounts.google.com.secure>
Date: Sat, Jan 27, 2018 at 9:28 AM
Subject: Resolve 8 security issues found on your Google account
To: johnsmith@google.com

Google

John Smith

8 security issues found on your account!

johnsmith@google.com

We've upgraded the Security Checkup to give you specific, personalized recommendations to strengthen the security of your Google Account.
Take the 2-minute checkup now to see the actions you should take to make your account more secure.

Take action

googlesecurityreport.exe

You received this email to let you know about important changes to your Google Account and services.
© 2018 Google Inc.,1600 Amphitheatre Parkway, Mountain View, CA 94043, USA
et:166

Does this email seem genuine or suspicious?

- Genuine
- Suspicious
- I am not sure